SECURITY 2040

ضمان أمن الاتصالات في عصر الحوسبة الكمومّية

إدارة المخاطر التي تعترض التشفير

مايكل ج. د. فيرمير (Michael J.D. Vermeer) وإيفان د. بيت (Evan D. Peet)



تصميم الغلاف: بيتر سوريانو *(Peter Soriano)*
صورة الغلاف: أدوبي ستوك/ساكميستيرك *Adobe Stock/sakkmesterke*

للمزيد من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني:
www.rand.org/t/RR3102

الملخّص والتوصيات

ينتظر العالَم أول أجهزة الحواسيب الكموميّة، التي يُتَوَقّع أن تُحدِث ثورةً في عالَم الحوسبة. فقد تُمَكِّنُها قوتها غير المسبوقة من تفكيك نظام التشفير الرقمي الذي تعتمد عليه بنية المعلومات والاتصالات التحتية الحديثة. من خلال اختراق ذلك التشفير، تستطيع الحوسبة الكموميّة أن تُعرِّض الاتصالات العسكرية والمعاملات المالية ونظام دعْم الاقتصاد العالمي للخطر.

يستكشف هذا التقرير تلك المخاطر من خلال تقييم، أولاً، مدى السرعة التي يُرَجَّح تطوير الحواسيب الكموميّة بها؛ وثانياً، مدى السرعة المرجحّة لتوحيد معايير التشفير الذي يمكنه مقاومة هجمات الحواسيب الكمومية، أي التشفير ما بعد الكمّ (postquantum cryptography [PQC])؛ وثالثاً، مدى السرعة المرجَّحَة لاعتماد التشفير ما بعد الكمّ ومدى اتّساع نطاق هذا الاعتماد. يخلُص التحليل إلى أنّ التهديد الذي يتعرّض له أمن بنية الاتصالات التحتية الحديثة هو أمر ملحّ ولكنه قابل للإدارة، ويقدّم المؤلفان توصيات إلى الحكومة الأمريكية للاستجابة.

يجري أصلاً سباقٌ بين الدول والشركات التي تحاول تطوير الحواسيب الكموميّة (وفي المقام الأوّل في الولايات المتحدة والصين والاتحاد الأوروبي، علماً أنّ عدداً من الدول الأخرى تسعى إلى تحقيق هذا الهدف أيضاً)، بالإضافة إلى أنّ عدداً من التطبيقات التجارية المتوقَّعة لا علاقة لها بالتشفير. قد لا تتوفّر الحواسيب الكموميّة القادرة على تقويض التشفير الحالي قبل عقْدٍ من الزمن على الأقل، غير أنّها تشكّل أصلاً مخاطر، وهذه المخاطر ستنمو مع مرور الوقت. إنّ حلول التشفير ما بعد الكمّ قيد التطوير إلا أنها ستحتاج إلى التحسين والتوحيد والتطبيق. سيكون هذا الانتقال صعباً وسيستغرق وقتاً طويلاً، وقد يمتدّ على مدى عقود من الزمن بشكلٍ محتمل. علاوةً على ذلك، يشكّل ظهور الحواسيب الكموميّة خطراً رجعياً، لأنّ المعلومات التي يتم نقلُها بأمان اليوم من دون التشفير ما بعد الكمّ، والتي قد يكون تمّ التقاطها وتخزينها وإنّما بدون فكّ تشفيرها البتة، قد يتمّ الكشف عنها بمجرّد ابتكار الحواسيب الكموميّة. تشكّل الفترة التي يُتوقَّع خلالها أن تعيق عملية التشفير تطوير الحوسبة الكموميّة نقطة ضعْف تتطلب منا احترازيّاً معالجتها اليوم.

وبهدف تقييم هذه الجداول الزمنية والخطر المرتبط بها، اعتمدنا مقاربة مختلطة الأساليب تشمل مراجعة الدراسات السابقة، ومراجعة آراء الخبراء، وإجراء دراسة استقصائية واسعة النطاق حول المستهلِكين. لقد هَدَفَت هذه المقاربة إلى تقييم الأحداث والمخاطر وحالات عدم اليقين المُرَجَّحَة وتقديم التوصيات في السياسات وتدابير التخفيف من المخاطر الملائمة. تتلخّص نتائج هذا البحث على النحو الآتي:

- يُتوقع أن تكون الحواسيب الكموميّة القادرة على استخدام تطبيقات التشفير متوفّرة، في المتوسط، بعد حوالي 15 عاماً، أي بحلول عام 2033 تقريباً. ومع ذلك، يقيّم الخبراء إمكانية حصول تطوّرات قبل ذلك الوقت وبعده على حدّ سواء.
- يُتوقع صياغة البروتوكولات المعياريّة للتشفير ما بعد الكمّ (PQC) وإصدارها في غضون الأعوام الخمسة المقبلة. يختلف الوقت المتوقّع لاعتماد بروتوكولات التشفير ما بعد الكمّ بشكل شبه كامل ولكن من المتوقّع عموماً أن يمتد إلى منتصف أو أواخر ثلاثينيات القرن الواحد والعشرين، وربما إلى ما بعد ذلك بكثير. ومع ذلك، من المتوقّع أن يستغرق الانتقال على نطاق الوطن أو العالَم الضروري لتطبيق البروتوكولات المعياريّة والتخفيف من الضعف الناجم عن الحوسبة الكموميّة عقوداً، وهي مدّة أطول بكثير من الوقت الذي قدّر الخبراء أنّه قد يتوفّر للمهمة.
- إذا لم يتم تطبيق التشفير ما بعد الكمّ (PQC) بشكلٍ ملائمٍ بتاريخ تطوير الحواسيب الكموميّة القادرة، قد يصبح من المستحيل ضمان المصادقة الآمنة وخصوصية الاتصالات من دون إحداث تغييرات كبيرة وتخريبيّة في بنيتنا التحتية. من المتوقّع ألّا تكون نقاط الضعف هذه أسوأ من نقاط ضعْف الأمن الإلكتروني الحاليّة من نواحٍ متعدّدة فحسب، بل ستكون من نوعٍ مختلف، موسِّعةً أنواع نقاط الضعف الإلكترونية.
- يتمتّع المستهلِكون بمستوى وعي منخفض بالحوسبة الكمومية بشكلٍ عام، وكذلك بمستوى وعي منخفض بالمخاطر المرتبطة بظهورها. ويصحّ هذا الأمر على امتداد الديموغرافيّات وحتى بين الفئة العمرية الأكثر معرفةً والتي تتراوح بين 18 و35 عاماً.
- تُظهر استجابات المستهلِكين لتهديدات الحوسبة الكموميّة المحتملة اتساقاً منطقيّاً، فكلّما اقترب التهديد، زادت الاستجابة. فضلاً عن ذلك، أشارَت دراسة استقصائيّة إلى أنّ بعض المستهلِكين قد يستجيبون على الأرجح للتهديدات الأمنية ويكافئون الشركات التي يتصوّرون أنّها تحمي أمنهم بشكلٍ أكثر ملاءمة.
- ومع ذلك، يشير ضمناً عدم وعي المستهلِكين بالحوسبة الكموميّة والمخاطر المرتبطة بها إلى أنّ المستهلِكين لن يشكّلوا على الأرجح الدوافع الأوّليّة لتغيير السياسات حول هذه القضيّة. ونتيجةً لذلك، ستبرز الحاجة إلى تأييد القيادة الفيدرالية حماية المستهلِك.

الاختصارات	
AES	Advanced Encryption Standard معيار التشفير المتقدّم
CA	certificate authority هيئة إصدار الشهادات
CFRG	Crypto Forum Research Group مجموعة أبحاث منتدى التشفير
CIO	chief information officer مدير المعلومات
CISA	Cybersecurity and Infrastructure Security Agency وكالة الأمن الإلكتروني وأمن البنية التحتية
FIPS	Federal Information Processing Standards معايير معالجة المعلومات الفيدرالية
GAO	Government Accountability Office مكتب المساءلة الحكومية
GCS	Google Consumer Surveys دراسات جوجل (Google) الاستقصائية حول المستهلِكين
GSA	General Services Administration إدارة الخدمات العامة
IAD	Information Assurance Directorate مديرية ضمان أمن المعلومات
IETF	Internet Engineering Task Force فرقة العمل المعنية بهندسة الإنترنت
IoT	internet of things إنترنت الأشياء
ISO	International Organization for Standardization المنظمة الدولية لتوحيد المقاييس
IT	information technology تكنولوجيا المعلومات
NAS	National Academies of Sciences الأكاديميات الوطنية للعلوم
NIST	National Institute of Standards and Technology المعهد الوطني للمعايير والتكنولوجيا
NSA	National Security Agency وكالة الأمن القومي
NSTAC	National Security Telecommunications Advisory Council المجلس الاستشاري لاتصالات الأمن القومي
NSTC	National Science and Technology Council المجلس الوطني للعلوم والتكنولوجيا
NTIA	National Telecommunications and Information Administration الإدارة القومية للاتصالات والمعلومات
NQCO	National Quantum Coordination Office مكتب تنسيق الشؤون الكموميّة الوطني
NQIA	National Quantum Initiative Act قانون مبادرة الكمّ الوطنية
NQIP	National Quantum Initiative Program برنامج مبادرة الكمّ الوطنية
OMB	Office of Management and Budget مكتب الإدارة والموازنة
OSTP	Office of Science and Technology Policy مكتب سياسات العلوم والتكنولوجيا
PKC	public key cryptography التشفير باستخدام المفتاح العام
PKI	public key infrastructure البنية التحتية للمفاتيح العامّة
PQC	postquantum cryptography التشفير ما بعد الكم
QIST	Quantum Information Science and Technology علوم وتكنولوجيا المعلومات الكموميّة
QKD	quantum key distribution تقنية توزيع المفاتيح الكموميّة
SCQIS	Subcommittee on Quantum Information Science اللجنة الفرعية لعلوم المعلومات الكموميّة
SEC	U.S. Securities and Exchange Commission لجنة الأوراق المالية والصرف الأمريكية
S&T	science and technology العلوم والتكنولوجيا
TLS	transport layer security أمان طبقة النقل

من خلال الجمع بين هذه النتائج وتقييمات الخبراء وتوصياتهم الأخرى، نرى أنّ التهديد ملحّ. ويُعتبر هامش الأمان ضئيلاً أو معدوماً لبدء مرحلة الانتقال إلى التشفير ما بعد الكمّ. سيؤثّر الضعف الناجم عن الحواسيب الكموميّة على كلّ الهيئات الحكومية والبنى التحتيّة الأساسيّة وقطاع الصناعة. ويشكل هذا تهديداً للأمن القومي يتطلب مقاربة منسّقة مركزياً على صعيد الدولة بأكملها للتخفيف من المخاطر. لقد اتخذت الحكومة الأمريكية مؤخراً عدداً من التدابير الهادفة إلى الحفاظ على مكانتها باعتبارها رائداً عالميّاً في علوم وتكنولوجيا المعلومات الكموميّة وضمان هذه المكانة، بما فيها تمرير قانون مبادرة الكمّ الوطنية (National Quantum Initiative Act) وتشكيل مكتب تنسيق الشؤون الكموميّة الوطني (National Quantum Coordination Office [NQCO])، ولكن لم يتّضح حتّى الآن ما إذا استجابت بشكلٍ ملائم للتهديد الذي تشكّله الحواسيب الكموميّة على أمننا.

يشبه التهديد الظروف المحيطة بالاستعدادات للانتقال إلى العام 2000 (Y2K) من نواحٍ عدّة. لقد نشأت مشكلة الانتقال إلى العام 2000، المعروفة أيضاً باسم "خلل الألفية" ("Millennium Bug")، من الخوف من حصول خللٍ في برمجيّات التقويم قد يتسبّب بفشل الحواسيب حول العالَم منتصف ليلة 31 ديسمبر/كانون الأوّل 1999، عندما أشارت الساعة إلى دخولنا العام 2000. وشكّل هذا الأمر خطراً مماثلاً لبنية المعلومات والاتصالات التحتية العالمية. كان أبرز الدروس المستفادة من الاستجابة لتحدي الانتقال إلى

العام 2000 أنّ القيادة الفيدرالية والشراكات اعتُبِرَت أساسيةً للنجاح، لا سيما التنسيق بين السلطة التنفيذية والرقابة من قبل حزبيْ الكونغرس. وأدّت هذه الأمور تباعاً إلى بروز شراكات ناجحة مع الولايات والمدن والمجموعات الصناعية، وصياغة التشريعات وإجراءات الفرص المفيدة، وتخصيص رأس المال البشري والموارد اللازمة لمساعدة الكيانات على الاستعداد.

يختلف التهديد الناتج عن الانتقال إلى العام 2000 عن ذلك التهديد الناتج عن الحواسيب الكموميّة بشكلٍ ملحوظ. لقد كان العالَم على علْمٍ بالموعد النهائي لإصلاح الضعف الناتج عن الانتقال إلى العام 2000، بينما نجهل مثل هذا التاريخ المؤكَّد لمعرفة وقت ظهور خطر الحواسيب الكموميّة. علاوةً على ذلك، على عكْس مشكلة الانتقال إلى العام 2000، التي هدَّدَت بفشل الأنظمة بالجملة من دون تدخُّلٍ بشري، يكمن التهديد الناجم عن الحواسيب الكموميّة في وجود نقطة ضعْف يستطيع خصم متطور وقادر استغلالها. ومع ذلك، يمكن تكييف المقاربة التي اعتُمِدَت للاستجابة لمشكلة الانتقال إلى العام 2000 مع الجهود المبذولة للتخفيف من المخاطر أثناء الانتقال إلى الحوسبة الكمومية.

لدينا ثلاث نتائج مُستخلصة رئيسيّة لما هو مطلوب لتستجيب الولايات المتّحدة للتهديد الناجم عن الحوسبة الكمومية:

1. اتخاذ تدابير لتحفيز اعتماد التشفير ما بعد الكمّ *(PQC)* بشكلٍ قويٍّ في أقرب وقت ممكن. سيكون الانتقال الواسع النطاق والملائم إلى التشفير ما بعد الكمّ الوسيلة الأكثر فعاليةً للتخفيف من الخطر الناجم عن الحواسيب الكموميّة. علاوةً على ذلك، **كلّما اقتَرَبَت إمكانية تطبيق معيار قابل للتشغيل المتبادل للتشفير ما بعد الكمّ على نطاقٍ واسع، قلّ الخطر المُقْبل.**
2. إدماج المرونة الإلكترونية وسرعة التشفير في البنية التحتيّة الرقمية. مع تكييف تطبيقات الأمن استجابةً للتهديدات الحالية المتطوّرة باستمرار على بنيتنا التحتية الأساسيّة وللتهديدات المستقبلية على حدّ سواء، مثل الحوسبة الكموميّة، يجب أن ننظر في كيفية جعْل تطبيقات الأمن الجديدة أكثر سرعة. وبشكلٍ محدّد، يجب أن تهدف الأنظمة الجديدة إلى (1) تحقيق التوافق المستقبلي مع تطوُّر معايير التشفير ما بعد الكمّ (PQC) ومستلزماته المتوقّعة الأكثر تطلباً، و(2) تطبيق النمطية (modularity) التي قد تسمح بتكييفٍ سريعٍ وغير مكلف للتشفير مع اكتشاف تهديدات أو نقاط ضعْف جديدة. **توفّر التغييرات المنهجيّة اللازمة للانتقال إلى التشفير ما بعد الكمّ فرصة لتطبيق تحسينات هيكلية في كيفيّة استخدام التشفير في أنظمة الاتصالات والمعلومات التي قد تُحَسِّن قدرتنا على الاستجابة للتهديدات الإلكترونيّة الحالية والمستقبلية على حدّ سواء.** يجب أن يكون الهدف الترادفي من الجهود الرامية إلى تعزيز اعتماد التشفير ما بعد الكمّ والاستعداد للحوسبة الكمومية إعادة هيكلة الأنظمة من أجل تمكين المزيد من المرونة الإلكترونية وسرعة التشفير.
3. الاستعداد لمستقبلٍ مجهول. لا تزال الجداول الزمنية لتطوير الحوسبة الكمومية غير مؤكدة للغاية، ولكنّ مستقبلاً غير مؤكد ليس بالضرورة مستقبلاً أقل أمناً. يجب أن تسعى الرسائل الموجهة إلى الجمهور بشأن المخاطر الناجمة عن الحواسيب الكموميّة إلى إيجاد حلّ وسطيّ بين المبالغة في التهديد والتجاهل المتهوّر للخطر الحقيقي. تمتلك الولايات المتحدة حلولاً للتخفيف من المخاطر، بحيث لن تؤدّي حتّى أسوأ السيناريوهات إلى نهاية أمن المعلومات الرقمية. **وفي أفضل السيناريوهات، قد يتحسّن الأمن الإلكتروني عالميّاً.**

يشكّل تطوير الحواسيب الكمومية ذات الصلة بالتشفير نوعاً جديداً من التهديد لأمن بنية الاتصالات التحتيّة الأمريكية. اليوم، يجد المهاجمون الإلكترونيّون الأذكياء طرقاً لتجاوُز أنظمة التشفير الهادفة إلى حماية المعلومات. وبدلاً من ذلك، ستَستَخدِم الهجمات الإلكترونية المُمَكَّنَة كمّومياً (quantum–enabled cyberattacks) جهازاً يهاجم أنظمة التشفير تلك مباشرة، مخترقاً بذلك ركيزة لأمن المعلومات. يُعتبر هذا تهديداً أمنيّاً كبيراً وملحّاً، وقد يكون العجز عن إيجاد حلولٍ له مدمراً لأمن المعلومات والأمن العسكري والسياسي والاقتصادي.

ومع ذلك، إذا تَصَرَّفَت الولايات المتحدة في الوقت المناسب، من خلال سياساتٍ ملائمة، واجراءات الحد من المخاطر، ومقاربة تشمل الحكومة بأكملها، وبحِسّ جَماعي بأنّ الأمور ملحّة، تتوفّر لها فرصةٌ لبناء بنية تحتية مستقبلية للاتصالات تضمن الدرجة نفسها من الأمان أو تكون أكثر أماناً من الوضع القائم. يمكن جني الفوائد الهائلة المُتَوَقَّعَة من الحوسبة الكموميّة مع تعزيز الخصوصية والأمن. تمتلك الولايات المتحدة الحلول والوسائل، وعلى الأرجح، الوقت الكافي لتجنب كارثة كمّوميّة ولبناء مستقبل أكثر أماناً، ولكن فقط إذا بدأت بالاستعداد الآن.

آخذين هذه المبادئ في الاعتبار، نقدّم التوصيات الواردة في الصفحة التالية للسلطة التنفيذيّة والكونغرس والمنظمات الفردية للنظر فيها. (تفاصيل هذه التوصيات متوفِّرة في الصفحات من 34 إلى 38.)

أبرز التوصيات

توصيات للسلطة التنفيذية

إذا كان البيت الأبيض يرغب في الحد من المخاطر الناجمة عن الحوسبة الكموميّة، فيجب أن:

- **يضمن قيام هيئة تنسيق مركزية بإيلاء التهديد أولوية كافية:** تتطلّب استجابة الحكومة الأمريكية وجود هيئة مُخَصَّصَة للاستجابة للتهديد الناجم عن الحوسبة الكمومية ومسؤولة عن تنسيق العمل في الحكومة وقطاع الصناعة. من غير الواضح حتى الآن ما إذا كان باستطاعة مكتب تنسيق الشؤون الكمومية الوطني (National Quantum Coordination Office [NQCO]) أن يولي اهتماماً كافياً للتهديد، بسبب وجود أولويات أخرى لديه، وبالتالي ينبغي على السلطة التنفيذية أن تنظر فيما إذا كانت هناك حاجة إلى هيئة أو مقاربة بديلة.

- **يضع معياراً لتسهيل الاعتماد:** الحد من عدد الخوارزميات النهائي الواجب توحيدها من قِبَل المعهد الوطني للمعايير والتكنولوجيا (National Institute for Standards and Technology [NIST]) ومتابعة وضْع معيار دولي. تماشياً مع معايير تقييم المعهد الوطني للمعايير والتكنولوجيا الحالية، يجب تصميم المعيار لتَجَنُّب تجزئة السوق، وزيادة قابلية التشغيل المتبادل (interoperability) إلى أقصى حد، وتسهيل الاعتماد على نطاقٍ واسع.

- **يفرض انتقال الحكومة إلى التشفير ما بعد الكمّ (PQC):** يتوجب على مديرية الأمن الإلكتروني في وكالة الأمن القومي (NSA Cybersecurity Directorate) النظر في فرْض انتقال الوكالات الحكوميّة، والبنى التحتيّة الأساسيّة والمنظّمات الأخرى إلى التشفير ما بعْد الكمّ (PQC). ويجب أن تضمن الإنفاذ المناسب وأن تمنح بعض الإعفاءات.

- **ينسّق بين الوكالات للدفع بالتغيير وتحسين الوعي:** توسيع تمثيل هيئة التنسيق المركزية لتشمل موظفين من عدد أكبر من الإدارات والوكالات في الحكومة الفيدراليّة. تكليفهم بأسرع وقت (1) بدعوة أصحاب الشأن في الحكومة والقطاع الخاص لزيادة الوعي ومعالجة الخطر الناجم عن الحواسيب الكموميّة، (2) بإصدار إرشادات محدثّة بشكلٍ متكرّر حول الانتقال إلى التشفير ما بعد الكمّ (PQC) وسرعة التشفير، و(3) بالدفع بتغييرات واسعة النطاق في مجال تكنولوجيا المعلومات.

توصيات للكونغرس

إذا كان الكونغرس يرغب في تعزيز الاستجابة للخطر الناجم عن الحوسبة الكمومية وزيادة الرقابة، فيجب أن يأخذ في عين الاعتبار ما يلي:

- **عقْد جلسات الاستماع لتحسين الوعي والرقابة:** يمكن لجلسات الاستماع في الكونغرس تعزيز الوعي حول الخطر الناجم عن الحوسبة الكمومية، وإطلاق الرقابة، ورصْد التقدُّم باتجاه الاستعداد للحواسيب الكموميّة. ينبغي أن تولي اللجان اهتماماً خاصاً للخط الفاصل غير الواضح بين منظّمات الأمن القومي والأمن غير القوميّ.

- **تحفيز الانتقال إلى التشفير في القطاعين العام والخاص:** تتضمن الخيارات التشريعيّة المُتاحة للكونغرس (1) وضْع المزيد من اللوائح حول الانتقال إلى التشفير ما بعْد الكمّ (PQC) وسرعة التشفير وزيادة مستوى فرضهما على الحكومة والبنى التحتيّة الأساسيّة، (2) تخصيص إضافي أو أكثر تركيزاً لرأس المال البشري والتمويل لجهود الحكومة المبذولة في مجال الانتقال، (3) توفير حوافز لشركات الأعمال للانتقال إلى التشفير ما بعد الكمّ، و(4) وضْع مخطّط إصدار الشهادات لتطبيق التشفير ما بعد الكمّ بشكلٍ ملائم.

توصيات للمنظمات الفردية

إذا رَغِبَت المنظمات في الحد من المخاطر، يجب أن تنظر في

- **تقييم الخطر المستقبلي والرجعي الناجم عن الحواسيب الكموميّة:** دمْج المخاطر الناجمة عن الحواسيب الكموميّة في تقييم المخاطر التنظيمية وإدارتها. تقييم نقاط الضعف الحالية والمستقبلية، بما في ذلك تلك الموجودة في المعلومات التي تمّ التقاطها أو قد يتمّ التقاطها الآن واستغلالها بعد أعوام.

- **جرْد استعمالات التشفير باستخدام المفتاح العام:** جرْد كل مكان داخل المنظّمة يُستخدم فيه التشفير باستخدام المفتاح العام، من قِبَل الشركاء، والجهات الموردّة من الأطراف الثالثة. سيحتاج كلّ طرف في نهاية المطاف إلى الانتقال إلى التشفير ما بعد الكمّ (PQC) بمجرد توفُّر معيارٍ ما.

- **بناء المرونة الإلكترونية وسرعة التشفير:** التخطيط لبناء مرونة إلكترونيّة وسرعة تشفير أكبر لتحسين الأمن الإلكتروني بمجمله وتسهيل عمليات الانتقال المستقبليّة إلى التشفير.

المقدّمة

لقد شكَّل التشفير باستخدام المفتاح العام (public key cryptography [PKC]) العمود الفقري للثقة في كافة الاتصالات الرقمية منذ ظهور الإنترنت. فقد سمح للأشخاص الذين نادراً ما يتقابلون شخصيّاً أو حتى الذين لا يتقابلون البتة، بتبادل المعلومات الهامّة والحسّاسة من خلال تفاعُلٍ رقميٍّ آمن. يسمح التشفير باستخدام المفتاح العام لطرفين بتبادل المعلومات فيما بينهما حصراً على قناة اتصال مرئية للآخرين بخلاف ذلك.

يوفّر التشفير باستخدام المفتاح العام الخصوصية والأمن اللازمين لتمكين مجموعة واسعة من التفاعلات الرقمية. ففي كلّ مرّة نتحقّق فيها من البريد الإلكتروني ونفتحه، أو نتصفّح حسابات مواقع التواصل الاجتماعي، أو نتسوق على مواقع التجارة الإلكترونية، أو ندفع مقابل الغداء مستخدِمين بطاقات الائتمان، أو نقوم بتحرير الوثائق المخزنة على السحابة، أو نعمل عن بُعد عبر الشبكات الافتراضية الخاصة، أو نسمح لتطبيقات هاتفنا النقّال بالتحديث تلقائياً، يمكّن التشفير باستخدام المفتاح العام كلّ طرف من الوثوق بالمعلومات التي يقدّمها الطرف الآخر. باختصار، إنّ التشفير باستخدام المفتاح العام، المعروف أيضاً باسم التشفير غير المتناظر (asymmetric cryptography)، هو ما يوفّر الأمن ويسمح بالثقة في الاتصالات الشبكية المفتوحة.

في التشفير باستخدام المفتاح العام، يمتلك كلّ مُستخدِم مفتاحين، أحدهما عام والآخر خاص. يبقى المفتاح الخاص سرّياً. لا يمكن فكّ تشفير أي رسالة مشفرة (أي، المختلطة رياضياً) بواسطة المفتاح العام إلا باستخدام المفتاح الخاص، وبالتالي يمكن نقلها بأمان عبر قنوات مُلاحَظَة. على الرغم من ارتباط المفتاحين العام والخاص رياضياً، ويمكن تقنياً التمييز ما بينهما عندما تكون المفاتيح صغيرة بما يكفي، إلّا أنّ المفتاح الخاص ظلّ آمناً حتى الآن لأنّ العمليات المطلوبة لاستخراج المفتاح العام، مثل تحليل العدد إلى عوامل وحلّ مشاكل اللوغاريتمات المنفصلة، كانت تمثّل تحدياً حسابياً.[1]

على الرغم من ذلك، تمّ عام 1994 التشكيك بقابليّة بقاء التشفير باستخدام المفتاح العام في المستقبل، عندما نَشَرَ عالِم الرياضيات بيتر شور (Peter Shor) ورقة يصف فيها كيف يمكن لجهاز نظري يدعى الحاسوب الكمومي أن يحلّ مشاكل تحليل العدد إلى عوامل واللوغاريتمات المنفصلة خلال فترة زمنية أقصر من المدّة التي تحتاجها الحواسيب التقليديّة، ممّا يجعل المفاتيح الخاصة ضعيفة (شور [Shor]، 1994).
غالباً ما تُقدّر المدة التي ستستغرقها الحواسيب التقليدية لتحليل الأعداد الشائعة الاستخدام في التشفير باستخدام المفتاح العام إلى عوامِل في نطاقات زمنية تعادل عمر الكون تقريباً. في المقابل، يمكن نظرياً لحاسوبٍ كموميٍّ قويٍّ بما يكفي أن يقوم بنفس المهمة في غضون أيام أو ساعات.

بما أنّ الحصول على مفتاح عام من مفتاح خاص بديهي ولكن يتعذّر القيام بالعكس حسابيّاً، يعمل التشفير باستخدام المفتاح العام خلف الستار في جميع الاتصالات الرقمية تقريباً حتى تاريخه، موفّراً الآلية التي تجعل الإنترنت آمناً. ستتحدى الحواسيب الكموميّة كلّ ذلك. إذا كان التشفير باستخدام المفتاح العام، وهو الآلية الحالية لجعل الإنترنت آمناً، يمتلك نقاط ضعْف يمكن لحاسوبٍ كموميٍّ استغلالها، قد يؤدي ذلك، نظرياً، إلى جعْل البنية التحتية الرقمية الحديثة غير قابلة للبقاء، لأنّه قد لا يبقى للاتصالات التي تتراوح بين رسائل البريد الإلكتروني الخاصة والمعاملات المالية وبيانات الأمن القومي أي خصوصية أو موثوقية مضمونة. فقد أطْلَقَت الورقة التي نَشَرَها شور سباقاً لابتكار حاسوب كمومي وأثارت الحاجة إلى تطوير نظام تشفير جديد لحماية الخصوصية في عصر ما بعد الكم على حدّ سواء.[2]

ستقوم الحواسيب الكمومية بعمليات حوسبة مختلفة اختلافاً جوهرياً عن عمليات الحواسيب الثنائية التقليدية (conventional binary computers). تُعتبر البِتّة (bit) أصغر وحدة بيانات في الحواسيب التقليدية (الثنائية)، وتعطى قيمة عدديّة إمّا عند وقْف التشغيل (0) أو عند التشغيل (1). في المقابل، تُعتبر البِتّة الكمومية (qubit) أصغر وحدة بيانات في الحوسبة الكمومية. تستفيد البِتّات الكمومية من ميكانيكا الكمّ (quantum mechanics)،[3] بحيث تُظهر المفاتيح التي تكون عند وقْف التشغيل (0) أو عند التشغيل (1) في الحوسبة التقليدية حالة تسمّى التراكُب (superposition)، أو نوعاً من الاندماج بين الحالتين في آنٍ واحد. تسمح هذه الظاهرة لحاسوب كموميّ بإجراء عمليات تتضمّن عدداً من البِتات الكمومية في آنٍ واحد، بدلاً من أن تكون متسلسلة. يمكن أن توفّر هذه القدرة الجديدة تحسينات هائلة في بعض عمليات الحوسبة، بما في ذلك تحليل العدد إلى عوامل وخوارزميات البحث في قواعد البيانات. إنّ هذه القدرة على تحليل العدد إلى عوامل بسهولة نسبية، والتي باتت مُمكنة بواسطة خوارزمية شور، ستَسمح للحواسيب الكمومية بمهاجمة دفاعات التشفير القويّة مباشرة، بطريقة تختلف نوعياً عن الهجمات الإلكترونية الحالية. تَستهدِف غالبية الهجمات الإلكترونية الحالية نقاط الضعف البشرية أو التقنية التي تسمح لمهاجمٍ بالالتفاف على الدفاعات. ستَستخدِم الحوسبة الكمومية القوة الحسابيّة الأولية لتجتاز دفاعات التشفير نفسها. وبالتالي، ستضيف نقطة ضعْف أخرى إلى نقاط الضعف التي تشوب الأمن الإلكتروني حالياً.

من الممكن نظرياً أن تُعرّض الحواسيب الكموميّة التطبيقات التي تستخدِم الإنترنت للخطر وتدمّر القدرة على

الاحتفاظ بالأسرار في شكلٍ رقميّ، ولكن يمكن الحؤول دون حدوث هذه النتائج بالكامل. تملك الولايات المتحدة الوقت والتكنولوجيا لتطبيق أنظمة تشفير جديدة لا يمكنها مقاومة الحواسيب الكمومية فحسب بل جعْل التفاعلات الرقمية المستقبلية آمنة كما هي الآن، إن لم تجعلها أكثر أماناً. سيتطلب ذلك استعداداً وتطبيقاً وإرادة سياسية.

إنّ الحواسيب الكمومية القادرة على إحداث فوضى في الاتصالات الرقمية هي، على الأقل على بُعد أعوام. في الأعوام الأخيرة، كانت إنجازات تكنولوجية تتحقق بوتيرة سريعة، ولكن ما زالت الحاجة تدعو إلى مزيدٍ من الإنجازات الكبيرة لجعل هذا الحاسوب أمراً واقعاً. على رغم عقود من البحث، لا يزال الجدول الزمني لظهور حاسوبٍ كموميٍّ يتمتّع بالقدرة الكافية لمهاجمة أي تطبيق عاديّ للتشفير باستخدام المفتاح العام غير مؤكد. علاوةً على ذلك، حتى عند ابتكار أوّل حواسيب كمومية تقترن بهذه القدرة، فمن المرجّح جداً أن يتطلّب تنفيذ مثل هذا الهجوم وقتاً كثيراً وتكلفة مرتفعة جداً في البداية. وسيتوجّب على المهاجمين تحديد أولويات الأهداف المحتملة بدقّة أثناء عملهم على تحسين التكنولوجيا والأساليب. بالإضافة إلى ذلك، ثمّة أساليب جديدة (أو أقل تطوّراً) بديلة لتطبيق التشفير باستخدام المفتاح العام قد تكون مقاوِمة للهجمات الكمومية. يُعدّ هذا التشفير باستخدام المفتاح العام بعد الكمّ، المشار إليه فيما بعد بالتشفير ما بعد الكمّ (PQC)، مجالاً بحثيّاً نشطاً في مجتمع التشفير ويتمتّع أصلاً بعدد من التطبيقات المعروفة. يقوم عدد من منظمات تطوير المعايير باختبار خوارزميات التشفير ما بعد الكمّ وتحليلها،[4] وإنّ المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology [NIST]) في خضم صياغة بروتوكولات معياريّة للتشفير ما بعد الكم. يفيد المعهد الوطني للمعايير والتكنولوجيا بتاريخٍ مستهدفٍ لإصدار معيار التشفير ما بعد الكمّ بين عامي 2022 و2024، وبعد ذلك يجب البدء بالانتقال الواسع إلى الأمن باستخدام البروتوكولات الجديدة. تعتمد معرفة ما إذا كان توحيد معايير التشفير ما بعد الكمّ سيتمّ آنيّاً وسيكون فعالاً على الخيارات التنظيمية والموارد والأولوية المؤسساتية الإجمالية الممنوحة للجهد.

وبهدف فهْم أرجحية الخلل المحتمل الناجم عن ظهور الحوسبة الكمومية وحجمه، يحتاج المرء إلى النظر في جدولَيْن زمنيين: (1) الجدول الزمني لتطوير حاسوبٍ كموميٍّ يقترن بالقدرة الكافية لمهاجمة التشفير باستخدام المفتاح العام، و(2) الجدول الزمني لتوحيد معايير التشفير باستخدام المفتاح العام الجديد الذي لا يكون ضعيفاً في وجْه الحوسبة الكمومية واعتماده. ستحدّد كيفية تطوُّر هذين الجدولين الزمنيين على مدى الأعوام والعقود القادمة ما إذا كان تطوير حاسوبٍ كموميٍّ يعطّل أمن الاتصالات الرقمية بشدّة أو ما إذا كانت آثاره ستتضاءل من خلال التطبيق الملائم والآنيّ للتشفير ما بعد الكمّ.

يعتمد تطوير الحوسبة الكمومية على الابتكارات العلمية والهندسية. إنّ هذه الابتكارات مدفوعة بالطلب على قدرات الحوسبة الكمومية الجديدة التي من شأنها تعزيز العلوم الأساسية والدفْع بالاستثمارات الخاصة والمنافسة الدولية واللوائح التي تسهِّل الإنجازات العلمية أو تعرقلها. في حين أنّ هناك عدداً من الأمور المجهولة في مسار تطوير الحواسيب الكمومية المستقبلي، يُتوقّع أن يصدر معيار تشفير ما بعد الكمّ قبل استخدام الحواسيب الكمومية على نطاقٍ واسع. ولكنّ توحيد المعايير ليس كافياً. فبعد التوحيد، سينبغي اعتماد التشفير ما بعد الكمّ، وكلّما حدث ذلك في وقت أقرب، زادت الفوائد. وفي حال كان الجواب على سؤال "متى سيتم تطوير الحواسيب الكمومية؟" أي شيء عدا "أبداً"، ستكون الولايات المتحدة عرضة لفك تشفير المعلومات الحسّاسة، ليس في المستقبل فحسب، بل مع أثرٍ رجعي. ونظراً لاستخدام الشبكات المفتوحة للتواصل، يُفترض أن يسجّل عدد من الكيانات الاتصالات المشفرة اليوم. يجعل التشفير باستخدام المفتاح العام هذه الاتصالات غير قابلة للقراءة في الوقت الحالي، ولكن بمجرد ابتكار حاسوب كمومي، يمكن فك تشفير أي بيانات تم التقاطها وتخزينها مسبقاً واستغلالها. ونتيجةً لذلك، قد تواجه المنظمات المعنية بنقْل المعلومات التي يجب أن تبقى سرية لفترة طويلة جداً خطراً كبيراً بسبب تطوير الحوسبة الكمومية في المستقبل. يجب أن يحفّز هذا الضعف اعتماد أي طريقة للتشفير ما بعد الكمّ سريعاً،[5] سواء تمّ اختيار تلك الطريقة لتكون معيار الصناعة أم لم يتم اختيارها.

على الرغم من التهديد، قد تتسبّب عوامل متعدّدة بالتأخير. أولاً، يُعَدّ اعتماد أساليب تشفير جديدة مكلفاً. بالإضافة إلى ذلك، في معظم الحالات، يجب أن تتواصل الأنظمة الجديدة مع أنظمة التشفير على شبكات أخرى، وقد يؤدي الاختبار غير الكافي للأساليب الجديدة إلى التغاضي عن نقاط الضعف، ممّا يؤدّي إلى التشكيك في الحماية الموعودة. نتيجةً لذلك، وقبل اعتماد أساليب التشفير الجديدة، يجب الانتظار إلى ما بعد الانتهاء من التقييم والاختبار المؤديين إلى توحيد المعايير. عادةً ما تكون عمليات الانتقال إلى التشفير فوضوية وبطيئة، وثمّة سبب كافٍ للاشتباه في أنّ الانتقال إلى التشفير ما بعد الكمّ سيكون صعباً بشكلٍ خاص. ستُستعمَل المنتجات المصمّمة والمصنوعة الآن باستخدام التشفير لعقود وستكون عرضة للهجوم الكمومي حتى يتمّ إيقافها، ما لم يتمّ تحديثها. بالإضافة إلى ذلك، من غير الواضح إلى أي مدى يدرك المستهلِكون التهديد الذي تمثله الحوسبة الكمومية للتشفير باستخدام المفتاح العام ومدى

اهتمامهم بأمن معلوماتهم. قد يؤثر وعي المستهلِكين على سرعة استثمارات الشركات في مجال إعتماد التشفير ما بعد الكمّ والطلب عليها.

لمعالجة الأسئلة المحيطة بالجداول الزمنية المستقبلية لتطوير الحوسبة الكمومية والتشفير ما بعد الكمّ واعتماد التشفير ما بعد الكمّ بعد التطوير، استخدمنا مقاربة بحثية مختلطة الأساليب. نظراً لأن السياسات التي تشمل استثمارات الحوسبة الكمومية، وتوحيد معايير التشفير ما بعد الكمّ، واعتماد التشفير ما بعد الكمّ تنطوي على عدم يقينٍ لا يمكن معالجته بالعلوم والإحصاءات التقليدية، نستخدم أسلوب استنباط آراء الخبراء لتوصيف الجداول الزمنية (والشكوك) للحوسبة الكمومية والتشفير ما بعد الكمّ. يُعتبر استنباط آراء الخبراء إجراءً رسميّاً وموثّقاً للحصول على الأحكام الاحتمالية وجَمْعها، وهو الأكثر ملاءمةً عندما تتخطى القرارات المطلوبة المعرفة الراسخة (مورغن [Morgan]، 2014؛ كولسن وكوك [Colson and Cooke]، 2018).

لقد أجرينا 15 مقابلة مع خبراء عامّين أو أكاديميين في مجال الحوسبة الكمومية والتشفير ما بعد الكمّ، بالإضافة إلى خبراء في القطاع من الشركات المشارِكة في تطوير الحوسبة الكمومية أو الشركات المهتمّة بأساليب التشفير المتقدمة مثل التشفير ما بعد الكمّ. اعْتَمَدَت المقابلات بروتوكولاً منظماً للحصول على آراء الخبراء الاحتمالية حول الجداول الزمنية للحوسبة الكمومية، وتطوير التشفير ما بعد الكمّ، والاعتماد المرجّح للتشفير ما بعد الكمّ. كما استنبطنا آراء الخبراء حول المخاطر المطروحة في السيناريوهات الافتراضية حيث يتمّ تطوير الحوسبة الكمومية قبل توحيد معايير التشفير ما بعد الكمّ، أو حيث يتمّ توحيد معايير التشفير ما بعد الكمّ ثمّ تظهَر الحوسبة الكمومية إما بعد وقت قصير أو بعد فترة زمنية أطول.

باستخدام المعلومات المكتسبة من خلال استنباط آراء خبرائنا، قمنا بعد ذلك بوضع دراسة استقصائيّة، وأرسلناها إلى عينة وطنية من الأفراد المجيبين، بهدف التأكّد من وعي المستهلِكين بالتشفير والحوسبة الكمومية، ومن كيفية استجابة المستهلِكين للحوادث الإلكترونية السابقة، ومن كيفية احتمال تفاعُل المستهلِكين مع تهديد الحوسبة الكمومية للخصوصيّة وأمن المعلومات. تقدِّم نتائج الدراسة الاستقصائيّة حول المستهلِكين رؤية حول كيفية تأثير هذا التغيير المحتمل على سلوك المستهلِكين وتنير مداولات الشركات التي تقرّر الاستثمار في التشفير ما بعد الكمّ واعتماده.

ماذا تعني ضمناً هذه النتائج بالنسبة إلى الوكالات والمنظمات التي تحاول تقييم مخاطرها الناجمة عن الحوسبة الكمومية وإدارتها؟ تشير البيانات إلى الحاجة إلى إيجاد حل وسطي بين المبالغة في التهديد أو التخويف منه والتجاهل المتهور للمخاطر الحقيقية. قد تواجه وكالات ومنظّمات متعدّدة حاليّاً مخاطر ناجمة عن الحوسبة الكمومية على أمن المعلومات وستنمو هذه المخاطر بمرور الوقت. قد يكون مستقبلٌ مع وجود الحواسيب الكمومية كارثيّاً لأمن المعلومات بطرق متعدّدة، ولكن، توجَد حلول من شأنها التخفيف من هذا الضعف إذا تم تطبيقها بطريقة مدروسة وآنيّة. علاوةً على ذلك، يوفِّر ظهور الحوسبة الكموميّة الذي يمكن التنبؤ به عدداً من الفرص لإعادة تصميم المقاربة الحالية لعمليات الانتقال إلى التشفير ما قد يؤدّي في نهاية المطاف إلى تحسين الأمن الإلكتروني وتسهيل عمليات الانتقال إلى التشفير المستقبلية. وأخيراً، لا تُشكّل الحوسبة الكمومية مخاطر أمنية فحسب، بل تعِد أيضاً بالابتكار العلمي والتقني. إنّ التهديد بأنها قد تخترق النماذج التي يعتمد عليها الإنترنت حقيقي ولكن يمكن مكافحته. إذا عملت الحكومات والشركات بشكلٍ جَماعيٍّ لمعالجة ضعفها، فقد تترقّب هذه التكنولوجيا الجديدة بفضول وأمل وإثارة، بدلاً منه بخوف.

يُقسَم هذا التقرير على النحو التالي. في القسم التالي سنراجع الدراسات السابقة وسنعرض خلفية عن التشفير بشكلٍ عام وعن التشفير باستخدام المفتاح العام على وجه التحديد،

لقد أجرينا 15 مقابلة مع خبراء عامّين أو أكاديميين في مجال الحوسبة الكمومية والتشفير ما بعد الكمّ، بالإضافة إلى خبراء في القطاع من الشركات المشارِكة في تطوير الحوسبة الكمومية أو الشركات المهتمّة بأساليب التشفير المتقدمة مثل التشفير ما بعد الكمّ.

والتقدُّم المحرز في مجال تطوير الحوسبة الكمومية، وطبيعة التهديدات التي تُشكّلها الحوسبة الكموميّة على التشفير. بعد ذلك، سنصف نتائج استنباط آراء الخبراء والدراسة الاستقصائية حول المستهلِكين، والمنهجية والبروتوكولات التي يتمّ وصْفها في الملحقات. وأخيراً، سوف نختتم بمناقشة تداعيات عملنا وتوصياتنا.

الخلفية

لفهم الدوافع التكنولوجية والسلوكية للخطر الذي تشكّله الحواسيب الكمومية على أمن المعلومات والتجارة، نظرنا في ثلاثة مجالات مختلفة ولكن مترابطة، وهي: تطوير الحواسيب الكمومية، وتطوير التشفير ما بعد الكمّ (PQC)، والتحدّيات التي ينطوي عليها اعتماد مقاربات تشفير جديدة. لقد راجعنا المنشورات التقنية، والتقارير الإعلامية، والأبحاث الأكاديمية، ومصادر أخرى ونلخّص نتائجنا المُستخلصة هنا.

الحوسبة الكمومية

على الرغم من أعوامٍ من البحث والاستثمار الكبير، لا تزال الحوسبة الكمومية تكنولوجيا ناشئة. لم يتم التوصل إلى إجماعٍ حتى الآن حول الطريقة الفضلى لتطبيق ركيزة الحوسبة الكموميّة وهي البِتّة الكموميّة (qubit). يمكن مقارنة حالة الحوسبة الكمومية الحالية بالوقت الذي كانت فيه الحواسيب التقليدية لا تزال تستخدم أنابيب التفريغ، قبل الانتقال إلى الحواسيب القائمة على الترانزستور (transistor–based computers). تتم متابعة عدد من هندسات البِتّات الكمومية، بما في ذلك البِتّات الكمومية فائقة التوصيل (superconducting qubits)، والبِتّات الكمومية الأيونية المخزّنة (trapped ion qubits)، وبِتّات اللّف المغزلي الكمومية (spin qubits)، والبِتّات الكمومية الفوتونية (photonic qubits)، والبِتّات الكمومية الطوبولوجية (topological qubits). غالباً ما تسير الأبحاث العلمية الأساسية وهندسة المعدّات الحاسوبية جنباً إلى جنب بينما تسعى المنظمات للتغلب على التحديات التقنية التي تواجه توسيع نطاقها واستخدامها (توزالين [Touzalin]، 2016). تتميز كلّ هندسة بنقاط قوة ونقاط ضعْف من حيث القدرة على تحقيق معدلات منخفضة من الأخطاء، وربْط عدد من البِتّات الكمومية، والسيطرة المثبتة مع مسارٍ لتوسيع النطاق. إنّ الهدف الطويل الأمد هو تطوير حاسوبٍ كموميّ عموميّ يتحمّل الخلل. حتى وقتٍ قريب، كان الهدف على المدى المنظور تطوير حاسوبٍ كموميٍّ متوسط النطاق يمكنه، ولأول مرّة، تحقيق التفوّق الكمومي أو الميزة الكمومية، أي قدرة الحوسبة على حلّ مشكلة محدّدة لا يمكن حلّها حتى بأقوى الحواسيب التقليدية (بليشر [Bleicher]، 2018). وقد تحقّق هذا الهدف عام 2019 عندما أعْلَنَت جوجل (Google) عن أول عرْض على الإطلاق للتفوّق الكمومي، مدّعيةً أنّ جهازها يستطيع أن يؤدّي في 200 ثانية مهمّةً يتطلّب إنجازها قرابة 10,000 عام باستخدام حاسوبٍ خارقٍ تقليديٍّ ومتطوّرٍ جدّاً (أروتي وآخرون [Arute et al.]، 2019).

تحتوي الدراسات السابقة على تقديرات للجدول الزمني المطلوب لابتكار حاسوب كمومي تختلف بشكل طبيعي بحسب كيفية تعريف الحاسوب الكمومي والمسار المعتمد لتطويره. في عام 2018، أصْدَرَت الأكاديميات الوطنية للعلوم (National Academies of Sciences [NAS]) أحد أكثر التقارير شمولاً حتى تاريخه عن تقدُّم الحوسبة الكمومية وتوقّعاتها، وشمل أهمّ المراحل والمقاييس الرئيسيّة والتكنولوجيات الواجب تتبّعها عند تقييم تقدُّم أبحاث الحوسبة الكمومية. خلُصَ هذا التقرير إلى أن تطوير حاسوب كمومي واسع النطاق يتطلّب أقلّه ثمانية إلى عشرة أعوام، ولكنّه لم يتنبأ بموعد بناء مثل هذا النظام فعليّاً وذلك بسبب عدّة أمور مجهولة. ويوثّق التقرير التحديات المتعددة الكامنة في تطوير حاسوب كمومي واسع النطاق (الأكاديميات الوطنية للعلوم [NAS]، 2018b). في الواقع، قد يشكّل تحديد مقدار قوّة الحوسبة لتطبيقٍ ما مقارنةً بالحواسيب التقليدية أو الهيكليات المتنافسة تحدّياً (بيشوب وآخرون [Bishop et al.]، 2017). إننا مهتمون بتشكيل فهْمٍ أفضل للجدول الزمني لابتكار حاسوب كمومي ذات صلة بالتشفير، والذي نعرّفه عموماً على أنّه تطبيق للحوسبة الكمومية المقترنة بالقدرات الكافية لاختراق عدد من التطبيقات الشائعة للتشفير باستخدام المفتاح العام في إطارٍ زمنيٍّ مفيد.[6]

بُذلت جهود متعدِّدة لتقدير موارد الحوسبة التي قد تلزم لاستخدام خوارزمية شور (Shor) لاختراق مختلف تطبيقات التشفير باستخدام المفتاح العام، والتي تستنتج عادةً أنّ حاسوب كمومي قد يحتاج ما بين مئات ملايين (محسني وآخرون [Mohseni et al.]، 2017) إلى مليارات (روتيلير وآخرون [Roetteler et al.]، 2017) البِتات الكمومية المادية. لا تزال هناك تطبيقات تتطلّب أكثر من 100 بِتّة كمومية، في حين استعمل التطبيق الذي استخدمته جوجل لإثبات التفوق الكمومي 53 بِتّة كمومية.[7] في عام 2009، كان بعض الخبراء يتوقعون أنّ الحواسيب الكمومية لن تستطيع حلّ مشاكل التشفير العملية قبل 15 إلى 20 عاماً، وسيحتاج الأمر من 20 إلى 30 عاماً قبل ابتكار حواسيب كمومية قويّة بما يكفي لاختراق خوارزمية RSA–2048 (وهو تطبيق شائع للتشفير باستخدام المفتاح العام) (موسى [Moses]، 2009). في الآونة الأخيرة، وثّق موسكا

(Mosca) عدداً من التقديرات المرتبطة بجهود معدّات حاسوبية معيّنة، وذكر أيضاً تقديره الاحتمالي الخاص عن فرصة واحدة من أصل سبع لاختراق خوارزمية RSA-2048 بحلول عام 2026، وفرصة واحدة من أصل اثنتين لاختراقها بحلول عام 2031 (موسكا [Mosca]، 2015). في الوقت نفسه، افترض بعض الخبراء أنّه قد يتبين في النهاية أنّ تطبيق حوسبةٍ كموميّةٍ بهذا الحجم غير ممكن عملياً. في حين يبدو أنّ هذه وجهة نظر الأقلية، تستخدم قضيتهم حجّة أنّ توسيع نطاق الهندسات الحالية قد لا يكون عملياً. (موسكفيتش [Moskvitch]، 2018؛ كالاي [Kalai]، 2016). ثمّة أيضاً احتمال أن تؤدي الإنجازات المفاجئة في المعدات الحاسوبية أو الخوارزميّات الكمومية المحسّنة التي تقلّل من متطلبات الموارد إلى تسريع جداول التطوير الزمنية.

كما هو متوقَّع، في محاولةٍ للتنبؤ بأي حالة مستقبلية لتكنولوجيا ناشئة، ثمّة قدر كبير من عدم اليقين. ومع ذلك، يُعتبر فهْم الجدول الزمني لتطوير حاسوب كمومي ذي صلة بالتشفير مهماً للغاية لتقييم الخطر، حتى مع وجود قدر كبير من عدم اليقين في أي من التنبؤات اليوم والتي يجب مراجعتها بمرور الوقت. ستحتاج التطبيقات الحالية للتشفير في الاتصالات إلى التكيّف مع قدرة الحوسبة الجديدة هذه مع تقدُّم التطوير، وخاصة حيث يتمّ استخدام التشفير باستخدام المفتاح العام.

التشفير

استُخدم التشفير (حرفيّاً "الكتابة المخفيّة") لضمان أمن الاتصالات والمعلومات عن طريق إخفاء محتويات الرسائل باستخدام الرموز منذ عصر الإغريق على الأقل، ويعود استخدامه في الولايات المتحدة على الأقلّ إلى الحرب الثورية (Revolutionary War) (فيبر [Weber]، 2013). ومن بين الهيئات الحكومية الحديثة الأكثر مشاركةً في توجيه استخدام التشفير وتوحيد معاييره وتطبيقه في الولايات المتحدة هي وكالة الأمن القومي (National Security Agency [NSA]) والمعهد الوطني للمعايير والتكنولوجيا (NIST). وغالباً ما تتكامل أدوار هذه المنظمات وتتعاضد في الأمور المتعلقة بالتشفير.

تشمل مهام وكالة الأمن القومي كلّاً من استخبارات الإشارات وضمان أمن المعلومات. أُعطيت وكالة الأمن القومي دور ضمان أمن المعلومات بشكلٍ رئيسيٍّ عام 1990 مع إنشاء مديرية ضمان أمن المعلومات (Information Assurance Directorate [IAD]). لقد قامت وكالة الأمن القومي مؤخراً بإعادة تنظيم هيكليتها، فحلّت مديرية ضمان أمن المعلومات وضمّت عدداً من أنشطتها لمديرية الأمن الإلكتروني (Cybersecurity Directorate) المنشأة حديثاً. كان دور مديرية ضمان أمن المعلومات الرئيسي، الذي تضطلع به اليوم مديرية الأمن الإلكتروني، حماية أنظمة المعلومات السرية وغيرها من أنظمة المعلومات ذات الصلة بالأمن القومي وتأمين الثقة في الفضاء الإلكتروني بشكلٍ عام من خلال بناء شراكات مع الحكومة وقطاع الصناعة والأوساط الأكاديمية بهدف تسويق تكنولوجيا ضمان أمن المعلومات ومنتجاته.[8] لقد وضعَت المعايير وشجّعت البائعين على الاستناد إلى تلك المعايير (وكالة الأمن القومي [NSA]، 2016). من أبرز الأمثلة الحديثة على ذلك كان تعريف مديرية ضمان أمن المعلومات لمجموعة خوارزميات الأمن القومي التجارية (Commercial National Security Algorithm Suite)، المعروفة أيضاً باسم المجموعة ب (Suite B)، والتي نُشرت لإعطاء إرشادات حول خوارزميات ومعايير التشفير الموافَق عليها للاستخدام في أنظمة الأمن القومي (لجنة أنظمة الأمن القومي [Committee on National Security Systems]، 2015). ويكمّل المعهد الوطني للمعايير والتكنولوجيا (NIST) عمل وكالة الأمن القومي في إدارة التشفير. فإنّ المعهد الوطني للمعايير والتكنولوجيا مسؤولٌ عن تطوير معايير التشفير، ومعايير معالجة المعلومات الفيدرالية (Federal Information Processing Standards [FIPS])، والمبادئ التوجيهية لحماية أنظمة المعلومات الفيدرالية للأمن غير القومي. تُستخدم هذه المعايير أيضاً على نطاقٍ واسعٍ خارج الحكومة لحماية المعلومات الحسّاسة وتعزيز التنمية الاقتصادية وقابلية التشغيل المتبادل على نطاق الوطن والعالَم (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2016a).

التشفير في الاتصالات

غالباً ما تُستخدم ثلاثة أنواع من التشفير في الاتصالات: التشفير بالمفتاح المتناظر (symmetric key cryptography)، ودالّات الهاش التشفيريّة (cryptographic hash functions)، والتشفير باستخدام المفتاح العام (PKC).[9] يتمّ في بعض الأحيان الجمْع بين هذه الأساليب لضمان الأمن. إنّها ليست ضعيفة بالقدر نفسه في وجه الحوسبة الكمومية.

في التشفير بالمفتاح المتناظر، يُستخدم مفتاح سرّي مشترَك واحد لتشفير رسالةٍ وفك تشفيرها على حد سواء. يتمّ جمْع المفتاح المتناظر مع البيانات لإنشاء رسالة مشفّرة غير مقروءة، ولا يمكن لأحد عكْس هذه العملية والحصول على الرسالة غير المشفرة سوى الشخص الذي يمتلك المفتاح المتناظر. فيجب أن يمتلك طرفا الاتصال هذا المفتاح، وبالتالي يتطلّب التشفير بالمفتاح المتناظر وجود بعض

الوسائل للتبادل الآمن للمفتاح لاستخدامه. وعادةً ما يتم استخدام التشفير بالمفتاح المتناظر لتشفير بياناتٍ بالجملة ولتشفير محتويات الرسائل.

على عكس التشفير بالمفتاح المتناظر، تُعتَبَر دالّات الهاش التشفيريّة دالات تشفيرية أحاديّة الاتّجاه، أي أنّه لا يمكن عكْسها. فعندما يتمّ تطبيق دالّة الهاش التشفيرية على رسالةٍ ما، ينشأ نصٌ أصغر بحجم ثابت، يُعرف باسم الخلاصة (digest) أو الهاشّ، ويكون فريداً لتلك الرسالة. وقد ينتِج أي تغيير في الرسالة، مهما كان صغيراً، هاشاً مختلفةً تماماً. تُستخدَم دالّات الهاش إلى حدٍّ كبيرٍ في الاتصالات للتأكيد على أنّه لم يتمّ تغيير رسالةٍ ما. (شينك [Shenk]، 2018).

وفي التشفير باستخدام المفتاح العام، يمتلك كلّ مستخدِم مفتاحين مترابطين رياضيّاً فيما بينهما. يمكن مشارَكة أحد هذين المفتاحين علانيّةً مع أيّ شخص ويُطلَق عليه على نحو ملائم اسم المفتاح العام *(public key)*. ويحتفظ المستخدِم بالمفتاح الآخر الذي يسمّى المفتاح الخاص *(private key)* سريّاً. فلا يمكن فك تشفير أي رسالة مشفّرة باستخدام المفتاح العام إلّا باستخدام المفتاح الخاص المُناظر. نتيجةً لذلك، يمكن لأي شخص يعرف مفتاح مستخدمٍ العام تشفير رسالة باستخدام ذلك المفتاح ويضمن تمكُّن الجهة المتلقية المقصودة التي تملك المفتاح الخاص من قراءة الرسالة وحدها. وبما أنّ المفتاحين مرتبطان رياضياً، فمن الممكن تحديد المفتاح الخاص من خلال المفتاح العام، والعكس صحيح. مع ذلك، من الناحية العملية، يبقى المفتاح الخاص آمناً لأنّه في حين ينطوي استخراج المفتاح العام من المفتاح الخاص على عملية سهلة حسابياً (مثل ضرْب عددين أوّليين كبيرين معاً)، تنطوي العملية العكسية للحصول على المفتاح الخاص من المفتاح العام على مشكلة صعبة جدّاً حسابياً (مثل العثور على العددين اللذين يمثلان عوامِل عدد كبير واحد). ونتيجةً لذلك، يمكن للمستخدمين إنشاء مفاتيحهم العامة ونشرها بسهولة واثقين إلى درجة معقولة بأنّه لا يمكن لأي شخص يراها الحصول على مفاتيحهم الخاصة وقراءة الرسائل التي تم تشفيرها باستخدام المفاتيح العامة (شينك [Shenk]، 2018).

غالباً ما يُستعمل التشفير باستخدام المفتاح العام جنباً إلى جنب مع التشفير بالمفتاح المتناظر ودالّات الهاش في بروتوكولات الاتصالات الشائعة، حيث يُستعمل التشفير باستخدام المفتاح العام لإنشاء مفاتيح متناظرة مشتركة بشكلٍ آمنٍ لتشفير الرسائل في حين تُستخدم دالّات الهاش لضمان سلامة الرسالة. يتيح الأمن الذي يوفّره التشفير باستخدام المفتاح العام للشبكات التي يتوجب فيها على كلّ مستخدِم امتلاك مفتاحين فقط، أي زوج من مفتاحي المستخدِم العام والخاص، للتواصل بشكلٍ آمنٍ مع أي مستخدِم آخر على الشبكة. بينما يعمل هذا على إصلاح بعض تحديات قابلية توسيع النطاق من حيث المبدأ، لا يزال يتوجّب على نشْر التشفير باستخدام المفتاح العام معالجة التحديات العملية لمصادقة المستخدِم وتوزيع المفاتيح. ويتمّ تخطّي هذه التحديات بمفهوم يسمّى البنية التحتية للمفاتيح العامّة (public key infrastructure [PKI]).

البنى التحتية للمفاتيح العامّة

إنّ البنية التحتية للمفاتيح العامّة (PKI) هي مُرَكَّب يُستَخدَم لتحديد الهويات في شبكة تستعمل التشفير باستخدام المفتاح العام (PKC). ففي بنيةٍ تحتيةٍ للمفاتيح العامّة، يتمّ إصدار بيانات الاعتماد المعروفة بالشهادات الرقمية التي تحتوي على هوية مستخدِمٍ متحقَّق منها ومفتاح عام لربط شخص أو جهاز أو منظمة بمفتاح عام معيّن.[10] يمكن لمستخدِمي الشبكة المشارَكة في اتصالات موثوقة من خلال تقديم شهاداتهم الرقمية، ما يسمح للآخرين على الشبكة بالتحقق من هويّاتهم وإرسال رسائل مشفّرة لهم باستخدام المفاتيح العامة. يتمّ إصدار هذه الشهادات من قِبَل أطراف ثالثة في الاتصال موثوق بها، هي هيئات إصدار الشهادات (certificate authorities [CAs])، والتي توفّر هذا التحقّق من الهويات. في حين قد تُفوّض هيئات إصدار الشهادات مسؤولية تسجيل المستخدِمين أو إصدار الشهادات إلى شركات تابعة، إلا أنّها عادةً ما تكون بمثابة ضامن الثقة لبنية التشفير باستخدام المفتاح العام التحتية. (الأمن الإلكتروني لطاليس [Thales eSecurity]، 2018).

تُعَدّ الشهادات الرقمية والبنى التحتية للمفاتيح العامّة الجزء الرئيسي الذي يُسهّل المصادقة على المُستخدِم حيثما يُستعمل التشفير باستخدام المفتاح العام، بما في ذلك على الإنترنت. تُسْتَخْدَم الشهادات الرقمية في مجموعةٍ واسعةٍ من التطبيقات والأنظمة بحيث يصعُب التعرّف عليها كلّها. وتشمل الأمثلة، على سبيل المثال لا الحصر، الخدمات المصرفية عبر الإنترنت، والبريد الإلكتروني، والألعاب عبر الإنترنت، والتجارة الإلكترونية والهواتف الذكية، والحوسبة السحابية. تُنشَر أيضاً الشهادات الرقمية والبنى التحتية للمفاتيح العامّة في التطبيقات الخاصة، مثل الشبكة الداخلية لشركة ما. وتُستخدم لضمان أمن توقيع الرموز (code signing)، والتحقّق من ملكية البرمجيات وسلامتها قبل تنزيلها وتطبيق نشْر مسارات التحديث الموثوقة وتمكينها على نطاقٍ واسع، مثل تلك المستخدَمة في أنظمة تشغيل الحواسيب والهواتف الذكية. باختصار، تُعتبر الشهادات الرقمية عنصراً أساسيّاً يسمح بمجموعة واسعة من الأنشطة المرتبطة ببنيتنا التحتية الرقمية الحديثة، وهي تستند إلى الصعوبة المفترضة

لاستخراج مفتاح خاص من مفتاح عام حسابيّاً. إذا ومتى استطاع حاسوبٌ كموميٌّ استخراج المفاتيح الخاصة في فترات زمنية قصيرة نسبياً، سيهدد الثقة في هذه البنية التحتية بأكملها وأمنها.

المخاطر الناجمة عن الحوسبة الكمومية

لن تؤثر الحوسبة الكمومية على جميع أنواع التشفير بالطريقة نفسها.[11] سوف تتيح الخوارزميات المعروفة للحواسيب الكمومية تحسين الأداء، على الأقل في عمليتين محددتين تثيران قلقاً خاصاً في مجال أمن المعلومات هما: تحليل العدد إلى عوامِل (شور [Shor]، 1994) وخوارزميات البحث في قواعد البيانات (غروفر [Grover]، 1996). ستقلّل خوارزميات البحث في قواعد البيانات الكمومية من قوّة المفاتيح المتناظرة ودالّات الهاش الأمنية الفعّالة، ولكن ربما بشكلٍ معتدلٍ وحسب. يمكن مواجهة أفضل الهجمات الكمومية المعروفة حالياً على أقوى بروتوكولات التشفير بالمفاتيح المتناظرة من خلال مضاعفة طول المفتاح المتناظر. وعلى نحو مماثل، يمكن مواجهة أفضل الهجمات الكمومية المعروفة حالياً على أقوى دالّات الهاش من خلال زيادة طول المفتاح بنسبة 50 في المئة (شينك [Shenk]، 2018). علاوةً على ذلك، هناك أدلة رياضية (على الرغم من عدم وجود دليلٍ صارم) على أنّ هذا هو الحد الأقصى لتحسين الأداء الذي يكون حاسوبٌ كمّوميٌّ قادراً عليه، أي أنّه لم يتمّ العثور على خوارزمية أكثر فعاليةً (زلقا [Zalka]، 1999). وبالتالي، يجب عدم تجاهُل الحد من الأمن في هذه الأساليب في مقابل حاسوبٍ كموميّ، ولكن لا تتطلب مضاعفة طول المفتاح الفعّال بشكلٍ عام تعديلاً في التحوّل النموذجي في تطبيق التشفير لضمان أمن الأنظمة ضد هجوم من حاسوبٍ كمومي.

يشكّل التحسين الكمومي في حل حسابات التشفير باستخدام المفتاح العام تهديداً أكثر أهمّية. يوفر استخدام مفاتيح أطول مزيداً من الأمن لمواجهة محاولات اختراق المفاتيح العامة، ولكن تتطلب المفاتيح الأطول أيضاً مزيداً من الموارد الحسابية لعمليات التشفير وفك التشفير الروتينية باستخدام تلك المفاتيح. تُغيّر الخوارزميات الكمومية توسيع نطاق الموارد لاختراق المفاتيح بحيث يتطلّب استخدام مفاتيح طويلة بما يكفي لتوفير أمن مكافئ في مواجهة حاسوبٍ كموميٍّ توفير موارد حسابية غير عملية للتشفير وفك التشفير باستخدام تلك المفاتيح بسرعة.[12] هذا هو السبب الذي يجعل تطبيقات التشفير باستخدام المفاتيح العامّة الحاليّة غير فعّالة في نهاية المطاف وغير عملية في الدفاع ضد حاسوبٍ كمومي (ولكوفر [Wolchover]، 2015).

يؤدّي ضعْف مخطّطات التشفير باستخدام المفتاح

> إذا ومتى استطاع حاسوبٌ كموميٌّ استخراج المفاتيح الخاصة في فترات زمنية قصيرة نسبياً، سيهدد الثقة في هذه البنية التحتية بأكملها وأمنها.

العام الرئيسية إلى فئتين من الخطر. تتبع الفئة الأولى من قدرة حاسوبٍ كموميٍّ على اختراق المفاتيح العامة مثل تلك المستخدَمة في الشهادات الرقمية في فترة زمنية قصيرة، ممّا يهدّد المصادقة. وتتبع الثانية من قدرة حاسوبٍ كموميٍّ على فكّ تشفير الاتصالات التي كانت آمنة ضد الهجمات في وقت الإرسال ولكن تمّ حفْظها في شكلٍ مشفّر، فيمكن بالتالي فكّ تشفيرها عندما يتوفّر حاسوب كموميّ. إننا نطلِق على الأولى مصطلح (فك التشفير) "الآني" *(just-in-time)*، وعلى الثانية "التقِط الآن واستغِلّ لاحقاً" *(catch now, exploit later)* أو باختصار "التقِط واستغِلّ" *(catch and exploit)*.[13] ترتبط هاتان الفئتان بمخاطر مختلفة وأولويات مختلفة للاستعداد، من حيث الأمور التي تشكّل نقاط ضعْف، والخطوات الواجب اتخاذها للتخفيف من نقاط الضعف، وتوقيت اتخاذ تلك التدابير للاستعداد.

المخاطر الناجمة عن فك التشفير "الآني" (Just-in-time risks)

يُحتمل أن تكون نقاط الضعف الناجمة عن فك التشفير "الآني" أكثر تخريباً لأنّها تميل إلى تقويض الثقة في تحديد الهوية والمصادقة في الأنظمة التي تستخدِم التشفير باستخدام المفتاح العام (PKC). على سبيل المثال، إذا تمّ استخدام حاسوبٍ كموميٍّ للحصول على المفتاح الخاص لهيئة إصدار شهاداتٍ جذر (root certificate authority)، قد تقوم جهّة فاعلة خبيثة بإصدار شهادات رقمية قد تُعرّف عن نفسها زيفاً على أنّها تقريباً أي كيانٍ كان على الشبكة. فيمكنها تزوير التوقيعات الرقمية المطلوبة لتحديثات البرمجيات الموثوقة وتحميل البرمجيات الخبيثة على الأجهزة، وانتحال صفة المؤسسات المالية للقيام بعمليات احتيالية أو تحويلات نقدية،

أو الوصول بشكلٍ موثوقٍ إلى الشبكات الأخرى التي تستخدِم البنية التحتية للمفاتيح العامّة (PKI). وحتى إذا لم يتمّ اختراق جذر الثقة مثل هيئة إصدار الشهادات (CA)، يمكن اختراق مفتاح كلّ مؤسسة العام المستخدَم للتوقيعات، على أساس كلّ حالة على حدة، مع تأثيرٍ أكثر محدودية.

لحسن الحظ، تماشياً مع هذا التصنيف، يجب على الأنظمة العُرضة لفك التشفير "الآني" مجرّد إجراء تغييرات قبل أن يُستَخدَم حاسوب كمّومي ذو صلة بالتشفير ضدها. قد تكون الهجمات التي تستغلّ هذا النوع من الضعف أكثر صعوبةً أيضاً في بعض الحالات لأنّ مشكلة التشفير قد تتطلّب حلّاً آنياً، وليس بعد ساعات أو أيام. فمن المحتمل أن تكون العواقب السلبية للضعف في وجه هجومٍ كموميّ أكثر تخريباً، ولكن يمكن تخفيفها تماماً إذا تم إصلاح نقطة الضعف في الوقت المناسب.

التَقِط الآن واستغِل لاحقاً (Catch now, exploit later)

يشير مصطلح التقِط الآن واستغِل لاحقاً إلى البيانات المرسلة التي ليس لها سِريّة مستمرّة (بالغة الخصوصيّة) (forward secrecy) في وجه الحواسيب الكمومية. يمكن اعتراض البيانات المشفّرة باستخدام التشفير باستخدام المفتاح العام (PKC) والمُرسلة قبل ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير، وعلى الرغم من تعذُّر قراءتها في وقت الاعتراض، يمكن فكّ رموز هذه البيانات لاحقاً وقراءتها بواسطة حاسوب كمومي. يُعتبر طول الفترة الزمنية التي يجب أن تبقى فيها

ترتبط هاتان الفئتان بمخاطر مختلفة وأولويات مختلفة للاستعداد، من حيث الأمور التي تشكّل نقاط ضعْف، والخطوات الواجب اتخاذها للتخفيف من نقاط الضعف، وتوقيت اتخاذ تلك التدابير للاستعداد.

المعلومات المُرسلة سريّةً العامل الأوّلي المُؤثّر على الخطر الناجم عن هذا السيناريو. إذا تمّ الآن إرسال بيانات يجب المحافَظة على سريّتها لمدة 20 عاماً، ولكن تم ابتكار حاسوب كمومي في غضون عشرة أعوام، فإن نقْل تلك البيانات الآن من خلال التشفير باستخدام المفتاح العام سيؤدي إلى خطر. تنتهي صلاحية قيمة بعض البيانات بسرعة (على سبيل المثال، رقم بطاقة ائتمان تمّ إلغاؤها)، في حين يكون لأنواع أخرى من البيانات تداعيات طويلة الأمد من حيث الخصوصية والأمن (مثل المعلومات الجينيّة التي تمّ جمْعها من طفل أصبح الآن في القوى العاملة). لا يمكننا أن نَصِف أو نعدّد بشكلٍ واثقٍ كلّ الطرق التي قد تكون ضارة في حال جعْل بيانات اليوم علنيّة بعد أعوام، ولكن قد تشمل الأمثلة على ذلك ما يلي

- المعلومات الشخصية المُحرجِة
- التاريخ الطبّي أو المعلوماتِ الجينيّة
- سجلات الأحداث الجنائية
- المعلومات التي تلحق الضرر بالعلامات التجارية (على سبيل المثال، الاتصالات التنفيذية أو بيانات تجارب الأدوية)
- الملكية الفكرية الحسّاسة، بما في ذلك الأبحاث المبكرة التي قد تنذر بسبل بحْث مستقبلية أو خرائط طريق تنموية
- أي معلومات مرسَلَة بين مراكز البيانات السحابية، بما في ذلك ربّما ما بين السحابات الآمنة المستخدَمة لنقل المعلومات السريّة
- مراسلات وزارة الخارجية (State Department) أو الاتصالات بين مختبرات وزارة الطاقة (Department of Energy)
- معلومات عن بروتوكولات الأمن المادي للمنشآت.

كلّما قَصُرت المدّة بين وقت إرسال المعلومات من خلال التشفير باستخدام المفتاح العام الحالي ووقت ابتكار حاسوبٍ كموميٍّ، ازدادت فائدة تلك المعلومات بالنسبة لجهة فاعلة منافسة أو خبيثة. وستؤثر عوامل أخرى أيضاً على قيمة المعلومات والخطر الذي تتعرّض له منظمة جراء الكشف عنها. لن تكون البيانات الخاملة (أي التي لم تُنقل) ضعيفة (ما لم تُقرصن من مصدرها سابقاً)، وقد تتوقّع عدّة منظمات أنّ بياناتها القديمة ستكون ذات أولوية منخفضة لفك تشفيرها من قِبَل مهاجمٍ يمتلك موارد محدودة. علاوةً على ذلك، بالنظر إلى احتمال أنّ الجهات الفاعلة القومية وحدها قد تمتلك الموارد اللازمة للوصول إلى حركة الشبكة والتقاطها ثم تخزين البيانات التي تمّ جمْعها من خلال التجميع الكتلي لأعوام عدّة، قد يصحّ أيضاً أن يكون الجمْع المستهدَف وحده ممكناً

بدلاً من الجَمْع "بنطاق الشبكة" ("dragnet collection") في حين يُعتقد أنّ الحواسيب الكمومية على بُعد أعوام عدّة. ومع ذلك، من المرجح أن ينمو الخطر الناجم عن فك التشفير بأثر رجعي مع مرور الوقت، وتوجَد منظمات تضع منهجيات لتقييم المخاطر التنظيمية الناتجة عن هذا التهديد (موسكا ومولهولند [Mosca and Mulholland]، 2017).

التشفير ما بعد الكم

إنّ التشفير ما بعد الكمّ (PQC) هو فرعٌ من التشفير باستخدام المفتاح العام (PKC) متعلق بخوارزميات التشفير المُقاوِمة لهجمات الحواسيب الكمومية. فبدلاً من استخدام تحليل العدد إلى عوامل أو اللوغاريتمات المنفصلة، الضعيفة في وجه خوارزميات الكم المعروفة، تستَخدِم تطبيقات التشفير ما بعد الكمّ عدداً من المقاربات الأخرى للتشفير باستخدام المفتاح العام التي يُتوقّع أن تكون آمنة حتى ضد الحواسيب الكمومية. تشمُل هذه المقاربات أنظمة قائمة على الشبكية (lattice–based)، وقائمة على الرموز (code based)، وقائمة على الهاش (hash–based)، ومتعدّدة المتغيرات، من بين أنظمة أخرى (المعهد الأوروبي لمعايير الاتصالات [ETSI]، 2015). تُخصَّص الآن عدّة مقالات وإصدارات المجلات الخاصّة (أيسو [Aysu]، 2018) ومؤتمرات (بي كيو كريبتو [PQCrypto]، 2018) لهذا الموضوع.

في حين يُبذل جهدٌ بحثيٌّ كبيرٌ حول هذا الموضوع، إلّا أنّ هذه الأساليب أكثر حداثةً وخَضَعت لاختبارات قليلة نسبياً مقارنةً بمقاربات التشفير المستخدَمة حالياً. فنظراً لاحتمال أن تُحدث العيوب نقاط ضعْف غير متوقَّعة، يجب أن تخضع مقاربات الأمن الجديدة بعد تطويرها لاختبار مكثّف من قِبَل مجتمع التشفير. ومن الممكن أن تكون هذه العملية طويلة ومعقّدة. تتعرّض المقاربات الجديدة التي تبدو واعدة لهجمات بحثاً عن نقاط ضعف فيها؛ وفي بعض الأحيان، يتم العثور على نقاط الضعف ويجب التخلّي عن أعوام من العمل. هذا ما حدَثَ مع مخطّطٍ قائم على الشبكية يسمّى سوليلوكي [Soliloquy]، تمّ تطويره عام 2007، بعد اكتشاف مؤلّفيه هجوماً كموميّاً فعالاً ضده (كامبل، غروفز وشيفيرد، [Campbell, Groves, and Shepherd]، 2014).

إدراكاً منها للتهديد المحتمل الناجم عن الحوسبة الكمومية، أعلَنت مديرية ضمان أمن المعلومات في وكالة الأمن القومي (NSA IAD) أنها ستستعِّد للانتقال إلى خوارزميات التشفير ما بعد الكمّ في بروتوكولات الأمن التي توصي بها (وكالة الأمن القومي [NSA]، 2015). وأوصت بوقف جهد الانتقال الجاري إلى التشفير بالمنحنيات الإهليلجيّة (elliptic curve cryptography) تحسباً لجهد توحيد مستقبلي لمعايير التشفير ما بعد الكمّ. بعد ذلك بوقت قصير، أعلَن المعهد الوطني للمعايير والتكنولوجيا (NIST) عن طلب ترشيحات لخوارزميات التشفير ما بعد الكمّ باعتبارها بدايةً لمحاولة تطوير خوارزمية تشفير ما بعد الكمّ واحدة أو أكثر وتوحيدها لِتُنشَر على نطاقٍ أوسع (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2016b). منذ الدعوة الرسمية إلى تقديم العروض، تلقّى المعهد الوطني للمعايير والتكنولوجيا الجولة الأولى والثانية من العروض وعقَد مؤتمراً حول هذا الموضوع في أبريل/نيسان 2018. يتمّ التخطيط حالياً لعقْد مؤتمر آخر حول توحيد المعايير وجولات اختيار إضافية، وتتوقّع المنظمة إصدار مسودة معيار التشفير ما بعد الكمّ بين عاميْ 2022 و2024 (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2018b). في حين يختبر عددٌ من هيئات المعايير الأخرى التشفير ما بعد الكمّ ويحلّله (بيسن [Pecen]، 2018)، يبدو أنّ معظم هذه المجموعات تترقّب نتيجة عملية المعهد الوطني للمعايير والتكنولوجيا. وفي حين يُطلَب إجمالاً من الحكومة الفيدرالية الأمريكية استخدام معايير المعهد الوطني للمعايير والتكنولوجيا، والتي عادةً ما تُفْرَض على شكل منشورات خاصة لمعايير معالجة المعلومات الفيدرالية (FIPS) وللمعهد الوطني للمعايير والتكنولوجيا، غالباً ما تَعتمد هيئات في القطاع وغيرها من هيئات المعايير هذه المعايير أيضاً في محاولةٍ للحصول على فوائد قابلية التشغيل المتبادل للتشفير للأعمال والتجارة الوطنية والعالمية. وفي حالات متعدّدة، تَعتمد المنظمة الدولية لتوحيد المقاييس (International Organization for Standardization [ISO]) هذه المعايير أيضاً (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2016a).

من المتوقّع أن تُصبح الخوارزميات وأنظمة التشفير الجديدة علانيةً وتُعَرَّض بشدة لهجمات من مجتمع التشفير على مدى أعوام قبل أن توصي هيئات المعايير باعتمادها بشكلٍ إضافيّ. وبعد هذه المرحلة، يجب على الصناعات والمنظمات إجراء حساباتها الخاصة حول الوقت الذي سيُعتبر فيه من الأكثر حرصاً خفْض تكاليف الانتقال للحماية من تهديد مستقبلي غير مؤكَّد.

الانتقال إلى التشفير

بمجرد وضْع معيارٍ ونشْره، تبدأ عملية طويلة لانتقال الأنظمة إلى المعيار الجديد. قد يتطلّب المعيار الجديد تغييرات هامّة عند عددٍ من النقاط في حزمة البروتوكولات[14] والتي تشمل تغييرات في البرمجيات أو المعَدّات الحاسوبية أو هيكليات البيانات المضمّنة. يجب أن تُقارِن الصناعات والمنظمات بين تكاليف استخدام معايير التشفير القديمة المحتملة

وتكاليف الانتقال إلى المعيار الجديد. قد ينطوي ذلك على تكاليف تحويل مرتفعة، إذ يجب تطوير برمجيات جديدة وشراؤها وتحسين المعَدّات الحاسوبية. غالباً ما يشكِّل تصوُّر تكاليف التحويل المرتفعة دافعاً لتأخر الانتقال في الصناعة (ليش، فيريس، وسكوت [Leech, Ferris, and Scott]، 2018)، وتاريخياً، تُقاس الجداول الزمنية لعمليات الانتقال إلى التشفير بالعقود (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2017). بالإضافة إلى ذلك، غالباً ما يبلغ عمر المعدات المشتراة حديثاً، لا سيما معدّات نظام الأمن القومي، 30 عاماً أو أكثر. وبالتالي، قد تؤخِّر المعدات التي تستخدِم معايير تشفير قديمة إدخال المعيار الجديد إلى أن يتمّ استبدال المعدات (مديرية ضمان أمن المعلومات [IAD]، 2016).

في حين تحدث عمليات الانتقال إلى التشفير بسرعة في معظم الأحيان لدى أكثرية المستخدِمين، غالباً ما تحتوي التحويلات الكاملة ذيولاً طويلةً للبلد (أو للكرة الأرضية) بأكمله في حين تَخَلَّفَ بعض المنظّمات. وفي منشور صادرٍ عن المعهد الوطني للمعايير والتكنولوجيا عن معايير معالَجة المعلومات الفيدرالية رقم 180–2 (NIST FIPS Pub 180–2) عام 2002، تمّ توحيد معيار جديد لدالات الهاش التشفيريّة، وهي خوارزمية الهاش الآمنة –2 (SHA–2) (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2002). وفي نوفمبر/تشرين الثاني 2016، كانت نسبة 35 في المئة من المواقع الإلكترونية لا تزال تستخدِم شهادات بمعيارٍ أقدم، ولم تتوقّف متصفحات الإنترنت الرئيسيّة عن العمل بالمعيار القديم إلّا حتى عام 2017 ("بحث فينافي: 35 في المئة من المواقع الإلكترونية لا تزال تستخدِم شهادات خوارزمية الهاش الآمنة –1 (SHA–1) غير الآمنة وتُعرِّض المستخدِمين للخطر"، ["Venafi Research: 35 Percent of Websites Are Still Using Insecure SHA–1 Certificate and Putting Users at Risk"]، 2016). عرّفت فرقة العمل المعنية بهندسة الإنترنت (Internet Engineering Task Force [IETF]) أمان طبقة النقل (Transport Layer Security [TLS])، وهو بروتوكول للاتصال الآمن عبر الإنترنت وشبكات الحاسوب، لأول مرة عام 1999 على أنّه أمان طبقة النقل – النسخة 1.0 (TLS 1.0) (فرقة العمل المعنية بهندسة الإنترنت [IETF]، 1999). وأُطلِق الإصداران اللاحقان لأمان طبقة النقل – النسخة 1.1 (TLS 1.1) وأمان طبقة النقل – النسخة 1.2 (TLS 1.2) في عاميْ 2002 و2008 على التوالي. وفي أكتوبر/تشرين الأوّل 2018، أفادت المتصفحات الرئيسية باستمرار استخدام أمان طبقة النقل – النسخة 1.0 وأمان طبقة النقل – النسخة 1.1 بنسبة 1 في المئة، وقدَّرَ مختبر آخر أنّ 94 في المئة من المواقع دعَمَت أمان طبقة النقل – النسخة 1.2. لا تخطِّط متصفحات الإنترنت الرئيسية لوقْف استخدام أمان طبقة النقل – النسخة 1.0 وأمان طبقة النقل – النسخة 1.1 تماماً قبل عام 2020، أي بعد أكثر من عقدين على نشْر معيار أمان طبقة النقل – النسخة 1.0 (برايت [Bright]، 2018). إن الانتقال من بروتوكول الإنترنت – النسخة 4 (IPv4) إلى بروتوكول الإنترنت – النسخة 6 (IPv6)، وهو بروتوكول الاتصالات الذي يحدّد الأجهزة التي تتواصل على الإنترنت، جارٍ منذ سبعة أعوام، ولكن حوالي 25 في المئة فقط من المستخدِمين يستخدِمون النسخة الجديدة (مجتمع الإنترنت [Internet Society]، 2018). وأخيراً، تمّ نشْر معيار التشفير المتقدّم (Advanced Encryption Standard [AES])، وهو معيار للتشفير بالمفتاح المتناظر، لأوّل مرّة عام 2001 (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2001). في دراسة استقصائية حديثة للمعهد الوطني للمعايير والتكنولوجيا، كان العام 2014 عام اعتماد معيار التشفير المتقدّم المتوسّط لدى المستهلِكين الذين شملتهم الدراسة من القطاعين العام والخاص. فقد أفاد بعض المجيبين بأنّهم اعتمدوا المعيار مؤخّراً أي عام 2018 (ليش، فيريس، وسكوت [Leech, Ferris, and Scot]، 2018). وبالنظر إلى أنماط الاعتماد الأخرى، من المرجّح استمرار عملية اعتماد المعيار الواسعة النطاق على المستوى الوطني لبعض الوقت.

تختلف الأسباب الجذرية لكلّ من الأمثلة المذكورة أعلاه بالنسبة إلى كيفية تطوُّر النظام أو المعيار أو تأخيره. لقد تمّ تأخير بعضها بسبب فشل تصميم أنظمةٍ لقابلية التطوّر والتوافق المستقبلي، بينما تمّ تسريع جداول زمنية أخرى فعلاً من خلال تغيير القواعد الصناعية أو إصدار نُسَخ أحدثْ توفِّر فوائد مُضافَة للمستخدِمين، مثل تحسينات الأداء والأمن المُحسَّن. يختلف بعضها من حيث طبيعته عن الأخرى وسيتأثّر بعوامِل مختلفة: فتحسين بروتوكول الإنترنت – النسخة 6 هو تحسين شبكة، على عكْس التحسينات الأخرى، التي هي تغييرات في البروتوكولات. ومع ذلك، تُذكر هذه الجداول الزمنية المختلفة معاً بهذه الطريقة لتوضيح أنّ عمليات الانتقال المماثلة في البنية التحتية تستغرق وقتاً طويلاً، وعادةً ما تَتطوّر على مدار عقود.

تقترن عمليات الانتقال المطوّلة هذه بتكاليف مرتبطة بالضعف في وجْه الهجمات الإلكترونية. يُعَدّ كلٌّ من العجز عن وقْف البروتوكولات القديمة والضعيفة أو الأمن الذي يصعب تحسينه والمضمّنة في أنظمة طويلة الأجل أمثلة على مخاطر الأمن الإلكتروني الناتجة عن عمليات الانتقال المطوّلة. بينما تُوفِّر المعايير الجديدة أمناً أفضل، تَستمرّ المنظمات في استخدام المعايير القديمة لبعض الوقت، حتى بعد تمكينها المعيار الجديد، لتمكين قابلية التشغيل المتبادل

مع مستخدِمين آخرين أو لأداء أفضل. ثمة فئة من الهجمات الإلكترونية تُعرف باسم هجمات خفْض إصدار البروتوكول (protocol downgrade attacks)، حيث يرغِم مهاجمٌ نظاماً على استخدام معيارٍ أقدم لم يتم إيقافه بعد، ثم يستغلّ نقطة ضعْف معروفة فيه. ويُعتَبَر بعض الهجمات الكبرى التي تَستغل نقطة ضعُف في مستخلص الرسالة – النسخة 5 (MD5)، وهي دالّة هاش شائعة، أمثلة أولية على ذلك. في عام 2008، عَرَض باحثون نقطة ضعْف في مستخلص الرسالة – النسخة 5 سَمَحَت لهم بتزوير شهادة شرعية من هيئة إصدار الشهادات (CA) (سوتيروف وآخرون [Sotirov et al.]، 2008). وفي عام 2012، استخدم مهاجمون نقطة الضعف هذه لتزوير التوقيع الرقمي لهيئة جذر في مايكروسوفت (Microsoft)، ما أتاح لهم تزييف تحديثات مايكروسوفت وتحميل برمجيات خبيثة على أجهزة ويندوز (Windows) (ستينون [Stiennon]، 2012). على الرغم من هذا الهجوم الكبير المعلَن عنه، استمر استخدام مستخلص الرسالة – النسخة 5 في أماكن أخرى وتسبّب بمشاكل حتى مؤخراً في عام 2017، عندما تم اختراق موقع التواصل الاجتماعي في أمريكا اللاتينية تارينغا (Taringa) بسبب استمراره في استخدام مستخلص الرسالة – النسخة 5 (لايدن [Leyden]، 2017). ويُعد هجوم برامج الفدية واناكراي (WannaCry Ransomware) مثالاً على تحدٍّ مختلفٍ في تطبيق الأمن في الأنظمة الطويلة الأجل. لقد قدّمت مايكروسوفت رُقعةً (تصحيحاً) لنقطة ضعُف أمنية في أنظمة ويندوز بعد فترة وجيزة من تنبيهها إليها عام 2017، غير أنّ تلك الأنظمة التي تجاوزَت عمرها الافتراضي لم تتلقَّ الرُقعة (التصحيح)، وتأثَّرت بالهجوم (لي [Lee]، 2017).

الانتقال إلى التشفير ما بعد الكمّ (PQC)

لن يُعرف نطاق الانتقال إلى التشفير ما بعد الكمّ (PQC) إلّا بعد إصدار البروتوكولات المعياريّة، ولكن من المحتمل أن يتضَمَّن تغييرات بعيدة المدى. فقد يَتطلب الأمر زيادة طول المفاتيح، وزيادة أوقات المعالجة وهيكليات جديدة للبيانات، والتي يمكن أن يكون أيّ منها غير متوافق مع المعَدّات الحاسوبية أو البرمجيات عبْر حزمة البروتوكولات. ينتشر التشفير باستخدام المفتاح العام (PKC) والبنية التحتية للمفاتيح العامّة (PKI) على نطاق واسع، وفي نهاية الأمر سيتعيّن على كلّ جهاز وشبكة تستخدمهما الانتقال إلى استخدام المعيار الجديد لتكون آمنة في وجه الحواسيب الكمومية. قد يتطلّب هذا الأمر قدراً كبيراً من الجهد لجرد كلّ مكان يُستخدم فيه التشفير باستخدام المفتاح العام، ثم فحْص توافق المكونات والبرمجيات الواسع مع المتطلبات الجديدة عن

حيث تكون مكوّنات المعَدّات الحاسوبية غير متوافقة، سيتوجّب استبدالها بمعَدّات حاسوبية ومكونات جديدة غير متطوّرة بعد، وسيستغرق كلّ ذلك وقتاً وسيتسبب بتكاليف قد تؤدي إلى مزيدٍ من التأخير في قرار الانتقال.

كثب. وحيث تكون مكوّنات المعَدّات الحاسوبية غير متوافقة، سيتوجّب استبدالها بمعَدّات حاسوبية ومكونات جديدة غير متطوّرة بعد، وسيستغرق كلّ ذلك وقتاً وسيتسبب بتكاليف قد تؤدي إلى مزيدٍ من التأخير في قرار الانتقال.

تؤدّي مثل هذه المشاكل المتعلّقة بعمليات الانتقال إلى التشفير إلى ازدياد الدعوات للتركيز على سرعة التشفير والمرونة الإلكترونية (أي مقاومة الفشل الذي تُسبِّبُه الهجمات الإلكترونية). تشير سرعة التشفير بشكل عام إلى الاعتراف بأن التشفير يُخترق بمرور الوقت مع تحسُّن قدرة الحوسبة، وتبرز الحاجة إلى بذْل جهودٍ لتغيير كيفية استهلاك الأنظمة للتشفير بشكل منهجي بحيث يمكن نشْر البروتوكولات الجديدة بسهولة أكبر، ومعالجة العيوب المكتشفة حديثاً بسهولة أكبر، وتحقيق قدر أكبر من قابلية التشغيل المتبادل بين أنظمة التشفير المختلفة. قد يشمل مصطلح سرعة التشفير ثلاثة أنواع: السرعة في الخوارزميات (القدرة على استخراج رموز جديدة)، والسرعة في البروتوكولات (القدرة على اختيار نسخة بروتوكول مختلفة، مثل تفضيل أمان طبقة النقل – النسخة 1.2 [TLS 1.2] على أمان طبقة النقل – النسخة 1.1 [TLS 1.1])، والسرعة في التطبيق (القدرة على تحديث البرمجيات التي تحتوي على عيبٍ أو استبدالها) (الأكاديميات الوطنية للعلوم والهندسة والطب [National Academies of Sciences, Engineering, and Medicine]، 2018a).

تترافق سرعة التشفير مع الفوائد المحتملة لتخفيض تكاليف الانتقال وازدياد الأمن بسبب سهولة الابتعاد عن العيوب الأمنية المكتشفة حديثاً، ولكنها تترافق مع تكاليف محتملة إذا تمّ التعامل معها بشكل سيء. يمكن للآليات التي تدعم سرعة أكبر أن تُدخِل بعجلةٍ مزيداً من التعقيدات، ممّا يصعّب على المشغّلين عملية الضبط الآمنة. في حال عدم تنظيم عدد الخوارزميات أو البروتوكولات المدعومة بعناية، يمكن ضبْط الأنظمة للسماح أو عدم السماح بالنُسَخ الضعيفة. كان هذا هو الحال بالنسبة إلى نقطة ضعْف فريك (FREAK) في أمان طبقة النقل، حيث كان بالإمكان ضبْط الأنظمة بطريقة تتيح لمهاجمٍ الاحتيال عليها لاستخدام خوارزمية ضعيفة (بوردوش وآخرون [Beurdouche et al.]، 2015). يُعتبر التحجّر (ossification) خطراً آخر محتملاً على السرعة. ويشير التحجّر إلى ظاهرة تكون فيها جوانب البروتوكول مرنة من الناحية التقنية ولكن، عمليّاً، غالباً ما تُستخدم بنفس الطريقة لدرجة أنّه يتمّ تجاهُل المرونة، ولا يتمّ تطوير أدوات جديدة لاستيعابها. يؤدّي استخدام هذه المرونة في نهاية المطاف إلى عدم توافق مع الأنظمة الأخرى، كما حدث عندما نُشِرَ بروتوكول أمان طبقة النقل – النسخة 1.3 (TLS 1.3) (سوليفان [Sullivan]، 2017). باختصار، في حين تقترن مقاربات تحسين سرعة التشفير بفوائد محتملة كثيرة، يجب تعزيز السرعة وتطبيقها بعناية لتجنّب الصعوبات المماثلة. ومع ذلك، وعلى الرغم من هذه التحديات، أوصِيَ بتطبيق أنظمة أكثر سرعةً من حيث التشفير بشكلٍ سليمٍ باعتبارها وسيلة ضرورية للغاية لتحسين أمن الشبكة بشكلٍ عام، وللتخفيف من التهديد الناتج عن الحوسبة الكمومية على وجه التحديد. وكما لاحَظ أحد المشاركين في ورشة العمل، إنّ "أفضل خط دفاع هو القدرة على تغيير الأمور" (الأكاديميات الوطنية للعلوم والهندسة والطب [National Academies, of Sciences Engineering, and Medicine]، 2018a).

تلَخِّص مناقشتنا هنا نتائج المقابلات المُستخلصة الرئيسية وتداعياتها على صانعي السياسات.

في غضون ذلك، يُرجَّح أن يستغرق الانتقال إلى التشفير ما بعد الكمّ وقتاً طويلاً ويكون مكلفاً ومحفوفاً بالتحديات. سيتمّ تطوير المنتجات والأنظمة وإنتاجها من دون معايير جديدة وقد تُستخدم لعقود متعدّدة، وربما إلى ما بعد تطوير حاسوب كمومي. علاوةً على ذلك، ستكون المنظمات التي يتوجّب الحفاظ على سريّة بياناتها لفترة طويلة جدّاً عرضة لمزيدٍ من الخطر نتيجةً لنقطة ضعْف من فئة "التَقِط الآن واستغِل لاحقاً" كلّما طال انتظارها لإجراء الانتقال.

النتائج والمناقشة

ملخص نتائج المقابلات

تُلَخِّص مناقشتنا هنا نتائج المقابلات المُستخلصة الرئيسية وتداعياتها بالنسبة إلى صانعي السياسات. لقد تمّ تنظيم المقابلات مع الخبراء المتخصّصين للتمكّن من الحصول على نتائج قابلة للقياس من خلال مناقشات كانت كيفيّة (وصفيّة) بطبيعتها بخلاف ذلك. بالإضافة إلى السياق والرؤى الناجمة عن مناقشة كيفية (وصفية) للقضايا ذات الصلة، أسفرَت المقابلات عن تقييمات كميّة لجداول التطوير الزمنية ونقاط الضعف. لقد تمكّنا بالاستناد إلى الخبرة من الحصول على متوسّطات تَصِف متى يَتوقّع الخبراء تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير، أو متى سيتم اعتماد التشفير ما بعد الكمّ (PQC). بما يتجاوز النتائج المُستخلَصة الرئيسية التالية، يُقدّم تقريرٌ كاملٌ لنتائج المقابلات الخمس عشرة التي أجريناها مع الخبراء والمنهجية التي استخدمناها في الملحقين A وB، على التوالي.

في حين تَعتمد نتائجنا المُستخلَصة الرئيسية على تجميع آراء الخبراء، تُقدِّم تفاصيل مقابلاتنا رؤية حول الاختلاف في آراء الخبراء. يُعتبر الاختلاف الملحوظ في آراء الخبراء بحد ذاته نتيجة أساسية تَصِف عدم اليقين الكامن في تقييمات الخبراء. لقد أظْهَرَت النتائج الكميّة والسياق المحيط في المقابلات على حدّ سواء درجة كبيرة من الاختلاف في رأي الخبراء حول ما هو ممكن وما يُرَجَّح أن يحدث. في بعض الحالات، تَختلف الآراء اختلافاً كبيراً؛ فعلى سبيل المثال، رأى بعض الخبراء أنّه يمكن تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير في وقت قريب أي بحلول عام 2022، بينما اعتقد البعض الآخر أنّ التطوير يحتاج إلى 20 عاماً على الأقل. بالإضافة إلى ذلك، ترافَقَ كلّ توقّعٍ لخبير بدرجة كبيرة من عدم اليقين. فعلى سبيل المثال، أفاد كلّ خبير بأفضل التقديرات والنطاقات لتوقعاته. وتُظهر النطاقات التي أفاد بها كلّ خبير أنّ كلّ خبير غير متأكد إلى حدٍّ كبير من الجدول الزمني للحوسبة الكمومية، والتشفير ما بعد الكمّ، والآثار

المحتملة لسيناريوهات التطوير المختلفة. لهذا السبب، نُحيل القرّاء المهتمّين إلى تفاصيل آراء الخبراء الموضّحة في الملحق A (ص. 41). ونُقدّم في الملحق B تبريراً شاملاً ومفصّلاً لمنهجيّتنا المُعْتَمَدة في استنباط آراء الخبراء واستخدام هذا الأخير في إنتاج التوصيات الواردة في هذا التقرير (ص. 53).

لقد أدى استنباط آراء الخبراء إلى استنتاج مفاده أنّه من المتوقع تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير بحلول عام 2033. ومع ذلك، اعتُبرت جداول زمنية أكثر تفاؤلاً وتشاؤماً ممكنة، مع اقتراح ستة خبراء أنّه من الممكن على الأقل أن يتمّ تطوير حاسوب كمومي ذي صلة بالتشفير قريباً أي بحلول عام 2023، بينما اعتقد نصف الخبراء أنّه من الممكن ألّا يتمّ ابتكار مثل هذا الجهاز البتّة.

وكذلك الأمر، عندما طُرِح سؤال عن متى يُرجَّح تطوير نظام تشفير قادر على مقاومة الهجوم الكمومي، كان أفضل تقدير قدّمه معظم الخبراء هو حدوث هذا الأمر في عام 2023. لاحَظ معظمهم أن خوارزميات آمنة كمومياً (بشكلٍ مفترض) موجودة بالفعل، ولكنّها غير موحَّدَة بعد للتطبيق على نطاق واسع. واعتَقَد أغلب الخبراء أن التشفير ما بعد الكمّ قد يتمّ وفقاً لجدول المعهد الوطني للمعايير والتكنولوجيا (NIST) الزمني، الذي يضع معياراً يُفترض أن يتمّ إكماله بين عامي 2022 و2024، ولكنّ الأمر غير مضمون. واعتقَد أحد الخبراء أنّ الاستجابات الآمنة فعلاً في وجْه الحوسبة الكمومية قد لا تتوفّر البتّة، لأنّ أيّ تشفير باستخدام المفتاح العام تمّ تطويره قد يتبيّن في نهاية المطاف أنّه ضعيفٌ في وجه قدرات الحوسبة الكمومية المستقبلية.

لقد اعتبَر الخبراء أنّ القضية الأكثر أهميّةً هي توقيت اعتماد التشفير ما بعد الكم. قُدِّر متوسط التقييمات المرجح لاعتماد التشفير ما بعد الكمّ شبه الكامل (أي أكثر من 95 بالمئة من المنظمات) بالنسبة للمنظمات الحكومية ومنظمات التكنولوجيا المتقدمة في منتصف ثلاثينيات القرن الواحد والعشرين، مع تَخَلُّف منظمات التكنولوجيا الأقل تقدماً بخمسة أعوامٍ تقريباً. على الرغم من هذا المتوسط، أظهرَت تقييمات الخبراء الفردية، مرّة أخرى، اختلافاً كبيراً، بحيث كانت التوقّعات متطرّفة لجهة إمكانية الاعتماد المبكر والمتأخر على امتداد الفئات ومع توقُّع قابلية اختلاف كبيرة، حتى داخل القطاعات، من حيث سرعة التطبيق وملاءمته. في المناقشة المحيطة، تمّ تقييم هذه القضية أيضاً مراراً على أنّها تعتمد بشكلٍ كبيرٍ على مجموعةٍ متنوعة من الأحداث الخارجية وقرارات صانعي السياسات والتي قد تؤدي إلى تغييرات كبيرة في معدّل الاعتماد.

نقاط الضعف الناجمة عن الحوسبة الكمومية

توفِّر الرؤى المكتسبة من مناقشة السيناريوهات الافتراضية في المقابلات مع الخبراء توضيحاً مفيداً عن التهديدات الحقيقية، ونقاط الضعف، والعوامل التخفيفيّة التي ستكون موجودة في مجموعة من السيناريوهات المستقبلية المحتملة. إننا نبدأ المناقشة بدمج النتائج حول نقاط الضعف المتوقَّعة، وملامح مخاطر القطاع، ومعدلات الاعتماد، والإجراءات المضادة والاستجابات المرجّحة للتوصّل إلى تقييمات موجزة عن المخاطر الحقيقية والتأثيرات الطويلة الأمد التي قد تكون متوقَّعة في كلّ من السيناريوهات. وبهذه الطريقة، نأمل أنّ نقدِّم صوراً أكثر اكتمالاً لما قد يبدو عليه المستقبل، مع تقديم مجموعات قليلة من القرارات والافتراضات، للتشديد على أهميّة التدابير التي يمكن اتخاذها الآن للتأثير إيجابياً على المستقبل. يبرُز عددٌ من النتائج المثيرة للاهتمام، بما في ذلك تصوُّر الخبراء بأنّ العواقب على مؤسستي الدفاع والاستخبارات ستكون الأقل خطورة من بين المجموعات الأربع التي سألنا عنها (وذلك لأسباب متنوعة). مرة أخرى، للاطلاع على مزيد من النتائج المفصّلة من المقابلات التي أجريناها مع الخبراء، نحيل القارئ المهتم إلى قسْم السيناريوهات في الملحق A (ص. 41).

السيناريو رقم 1: مفاجأة الكم

في السيناريو رقم 1، الذي نُعنونِه "مفاجأة الكم"، يتمّ ابتكار حاسوب كمومي ذي صلة بالتشفير ويتمّ استخدامه قبل إصدار معيار للتشفير ما بعد الكمّ (PQC)، إمّا نتيجةً لبرنامج سريّ كبير أو بسبب قفزات مفاجئة في القدرات ناتجة عن التقدّمات والابتكارات في العلوم والهندسة الأساسية، يليها "سباق حتى النهاية". وتجدر الإشارة إلى أنّ البعض قد قيَّم أنّه من غير المرجّح جداً تطوير حاسوب كمومي واسع النطاق في السرّ، ما يعني ضمناً أنّ افتراض حدوث هذا الأمر قد يكون غير مُرَجَّح (مجموعة عمل التشفير [Encryption Working Group]، 2019). ومع ذلك، يعود هذا الأمر جزئياً إلى جهود التطوير الكبيرة المُحَفَّزَة بالتطبيقات المتوقعة التي لا علاقة لها بالتشفير، والتي قد تزيد أيضاً من احتمال حدوث قفزات مفاجئة في القدرات. في نهاية المطاف، نقيّم أنّ احتمالية حدوث هذا السيناريو منخفضة، ومع ذلك، قد يكون لحدوثه عواقب كبيرة، وبالتالي اخترنا أن نستفهم من الخبراء عن المخاطر المرتبطة به.

لا يوجد أي نظيرٍ واضحٍ لهذا السيناريو في التاريخ الحديث، وستكون العواقب خطيرة. اعتقد الخبراء أنّه في حال حدث ذلك من المرجّح أن تفشل القدرة على المصادقة على الهوية على الشبكات الرقمية وضمان الاتصالات الآمنة. فقد

قال أحدهم في معرض وصفه السيناريو؛

> أعْتقِد أنّ السيطرة على الهويّة، أي الهوية المحمية بالتشفير، قد فُقِدَت. وإمكانية عزل القناة بالتشفير فُقِدَت. وبذلك تصبح كلّ الاتصالات شفافة، وتصبح الهوية الضرورية للتمكّن من السيطرة الكاملة متاحة بسهولة.

في الواقع، اعتقد عدد من الخبراء أنّ أهمّ تهديد كان فقدان الهوية المصادَق عليها، مشيرين إلى أنّ المهاجمين قد يواصلون السيطرة على جذور الثقة في النظام، مثل المفاتيح الخاصة لهيئات إصدار الشهادات (CAs) الجذر، ما يؤدي إلى فقدان السيطرة التام في معظم الأنظمة الشبكيّة: "عليك أن تستهدِف أصول السيطرة، وهي الهوية. وإذا حصلْتَ عليها، فستحصل على كل شيء." كان من المتوقع أن تكون الأهداف العالية القيمة مثل شبكة جمعية الاتصالات المالية بين المصارف على مستوى العالَم (نظام سويفت [SWIFT network]) للخدمات المالية عرضة للخطر. أمّا الأهداف الدفاعيّة والاستخباراتيّة فكان من المتوقَّع أن تبدي درجة من الحماية، ولكن كان من المتوقع أن تتوفّر لمعظم المنظمات الأخرى فرصة ضئيلة لحماية أنظمة معلوماتها.

يمكن لهجمات إلكترونية مُتَّسقة ومتكرِّرة على مدار أشهُر أو أعوام، وخاصةً إذا بَقِيت غير مُكْتَشَفَة لبعض الوقت، أن تعطّل التجارة والعمليات المصرفية الرقمية، وتتسبّب بأضرار كبيرة وفقدان الثقة في السجلات الحيوية، وتقوّض التشغيل الموثوق به للبنى التحتية والاتصالات الأساسية. قد يسمح فقدان المصادقة في توقيع الرموز للمهاجمين بتوزيع برمجيات خبيثة على نطاقٍ واسع. في حين أنّ انهيار الكيانات المؤسساتي المنهجي مثل شبكة الطاقة الكهربائية أو النظام المالي مستبعدٌ نظراً للتخطيط والتنسيق والموارد المطلوبة لتنفيذ هجمات متتابعة وسريعة باستخدام تكنولوجيا الحوسبة الكمومية غير الناضجة، قد لا يزال من الممكن حدوث أضرار وتعطيل واسع النطاق. بما يتجاوز هذه الأعطال القصيرة المدى، فإنّ العواقب الناتجة عن فقدان الاتصالات الآمنة وفك تشفير الاتصالات الحديثة قد تتسبّب بنقاط ضعْف غير معروفة الحجم في المستقبل لأنّه تمّ استغلالها.

حتى ولو تمّ تنفيذ عددٍ قليلٍ من الهجمات أو وقَعَت أضرارٍ فعليةٍ طفيفة، قد تكون العواقب السلبية للاستجابة لمفاجأة الكمّ هذه كبيرة. فقد يتمّ فصْل الأنظمة الأساسية عن شبكة الإنترنت لفترات من الوقت احترازياً، وقد تتلاشى الثقة في المؤسسات. قد يكون للتدافع على تطبيق التشفير ما بعد الكمّ بسرعة عواقب طويلة الأجل من حيث التطبيق السيئ وإدارة الرُقَع (التصحيحات) المكلفة، على مدار أعوام عدّة. وبالتالي، ستضيع الفرصة للانتقال الفعال والقوي الذي يسمح بالمزيد من الفعالية وقابلية التشغيل المتبادل وسرعة التشفير.

ومع ذلك، قد لا يُنهي هذا السيناريو الكارثي أمن الاتصالات الشبكية بالكامل. بدلاً من ذلك، نتوقع حدوث أعطال وتعديلات تكيّفية قصيرة الأجل، ومجموعة من الأنشطة للتخفيف من نقاط الضعف، وفترة طويلة من التعامل مع تداعيات اختراق المعلومات الحسّاسة، لنستقرّ في النهاية في بيئة أقل أمناً وأقل يقيناً تبقى فيها الأمور على حالها.

السيناريو رقم 2: يسبق معيار التشفير ما بعد الكمّ (PQC) الحواسيب الكمومية ذات الصلة بالتشفير بفترة وجيزة

في السيناريو رقم 2، يتم ابتكار حاسوب كموميٍّ ذي صلة بالتشفير واستخدامه في غضون بضعة أعوام بعد إصدار معايير التشفير ما بعد الكمّ (PQC). في حين أنّ المنظمات التي تولي أمن المعلومات أولويّةً كبرى، مثل وكالات الدفاع والاستخبارات والجهات المزوِّدَة للبنية التحتية الأساسية، قد اعْتَمَدَت بالفعل التشفير ما بعد الكمّ، فإنّ معظم المنظمات الأخرى لم تفعل ذلك. قال أحد الخبراء، "أعتقد أنّ فكرة قدرتها على شراء الأنظمة التي تحتاج إليها ونشْرها في غضون ثلاثة أعوام من تاريخ توحيد معايير التشفير ما بعد الكمّ، شبه معدومة." ستبقى نقاط ضعف كبيرة قائمةً على امتداد القطاعات.

ولكن، في هذا السيناريو، تتوافر حلول أمن مناسبة في حالات متعددة، بما في ذلك عدد من بروتوكولات تكنولوجيا المعلومات (IT) الأساسية مثل أمان طبقة النقل (TLS) والتي ستنتقل بسرعة لتشمل التشفير ما بعد الكمّ. اعتقد الخبراء أنّ فرقة العمل المعنية بهندسة الإنترنت (IETF) ومجموعة البحث التابعة لها، وفرقة عمل أبحاث الإنترنت (Internet Research Task Force)، ومجموعة أبحاث منتدى التشفير (Crypto Forum Research Group [CFRG]) ومنظّمات مماثلة أخرى قد تَقْبَل خوارزميات المعهد الوطني للمعايير والتكنولوجيا للتشفير ما بعد الكمّ (NIST PQC) المعياريّة وتدمجها بسرعة في البروتوكولات التي تديرها. ستتوفّر هذه البروتوكولات على الإنترنت بسرعة، حتى ولو كان التخلّي التدريجي عن النُسَخ القديمة سيستغرق عقوداً. وبمجرد ابتكار حاسوب كمومي، ستدرك المنظمات بسرعة الحاجة إلى هذه الحلول وقد تنتقل إلى تطبيقها.

من الناحية المثالية، ستتيح سهولة توافر الحلول الأمنية المعياريّة المُمَكِّنة من التشفير ما بعد الكمّ درجة كبيرة من قابلية التشغيل المتبادل واعتماداً أسرع، ممّا يؤدّي إلى التخفيف من الأعطال الرئيسية المتوقّعة في السيناريو رقم 1، حتى ولو تسبّبت الهجمات الإلكترونية الرئيسية ونقاط الضعف الناتجة عن الاتصالات المُلتقطة مؤخّراً بمشاكل كبيرة. والسؤال هو بأي سرعة ستعتمد المنظمات التشفير ما بعد الكمّ والبروتوكولات الجديدة بمجرد توفُّرها. تاريخياً، اعتَمَد عدد من منظمات

"الانتقال الباكر" معايير البروتوكولات الجديدة بسرعة بمجرد إصدارها، بينما قد تستغرق الجهات المتأخّرة في الاعتماد أعواماً. ونظراً لحداثة هذا الانتقال وتعقيده ونطاقه، قد تكون جهات الانتقال الباكر ضعيفة أيضاً، ولو بدرجة أقل، حتى بعد تطبيق التشفير ما بعد الكمّ في الأنظمة الأوّلية. سيساعد اتخاذ إجراءات لتحفيز اعتماد التشفير ما بعد الكمّ بشكلٍ أسرع وأقوى بمجرد توفُّر معيارٍ في التخفيف من الخطر في هذا السيناريو.

السيناريو رقم 3: يسبق معيار التشفير ما بعد الكمّ (PQC) الحواسيب الكمومية ذات الصلة بالتشفير بفترة طويلة

في السيناريو رقم 3، يتمّ ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير واستخدامه بعد حوالي عقْدٍ على إصدار معيارٍ للتشفير ما بعد الكمّ (PQC). يُفترض في هذا السيناريو أنّ الانتقال الواسع النطاق إلى التشفير ما بعد الكمّ قيد التطبيق. ولكن، باتباع الأنماط التاريخية، لا يزال عدد كبير من المنظمات متخلفاً في مجال تحديث أمنه. ولا يزال عدد من المنتجات الطويلة الأجل أو التي يصعب تحديثها يستخدم تشفيراً ما بعد الكمّ ضعيفاً، وقد انتَظَر بعض المنظمات اعتماد التشفير ما بعد الكمّ "ضمنياً" خلال دورات إعادة تنشيط تكنولوجياته العادية.

تمّ تقييم السيناريو رقم 3 على أنّه الأقرب إلى وضْع ضعْف الأمن الإلكتروني القائم، على الرغم من أنّ معظم الخبراء أشاروا إلى أنّ هذا السيناريو قد لا يزال على الأقل أسوأ من الوضع الحالي بقليل. وعلى الرغم من وجود عقْدٍ من الزمن للاستعداد، اقْتَرَحَت سابقة تاريخية أن الانتقال إلى التشفير ما بعد الكمّ قد لا يزال غير مكتمل. فقد قال أحد الخبراء: "حتى بعد عشرة أعوام، لا تزال هناك، تاريخيّاً، بعض الأمور (التي) بقِيَت عالقة ولم يوليها أحد اهتماماً كبيراً، والتي قد تشكّل نقطة ضعْف محتملة". قد تبقى أنظمة متعدّدة تمّ نشْرها باستخدام تشفير ضعيف قيد التشغيل لأعوام عديدة في المستقبل، لا سيما في الحالات التي تتمتّع فيها المنتجات بدورات تطوير ونشْر طويلة وفي الحالات التي قد لا يُبدّي فيها المصنعون الأمن في وجْه الحواسيب الكمومية بشكل استباقي. علاوةً على ذلك، ستوفر نقاط الضعف المتبقية هذه ناقلات هجمات إضافية ممكَّنة بواسطة حاسوب كمومي، تضاف إلى تلك المتوفّرة اليوم.

لقد اعتقد الخبراء أنّ السيناريو رقم 3 هو أفضل السيناريوهات. قد لا يكون معيار للتشفير ما بعد الكمّ متاحاً وعملية الانتقال جارية في الوقت الذي يتمّ فيه ابتكار حاسوب كمومي فحسب، بل قد تُتاح للولايات المتحدة أيضاً الفرصة والحافز لاتخاذ بعض الإجراءات الاستباقية المفيدة للغاية لتحسين بنية التشفير التحتية بشكل عام. يمكن بدء الانتقال إلى التشفير ما بعد الكمّ مع ضمان وقتٍ كافٍ لتمكين انتقال قوي وغير متسرّع. إذا أُخِذَ التهديد الناتج عن الحواسيب الكمومية على محمل الجد بما فيه الكفاية، يمكن للمنظمات أن تدفع جماعياً بحلول التشفير ما بعد الكمّ المطبَّقة بشكلٍ آنيٍّ وملائم، وتدمجها في إدارة الأمن طوال دورة الحياة، والاستفادة من الفرصة المتاحة جراء الانتقال لبناء تشفير أكثر سرعةً في أنظمتنا. ونتيجةً لذلك، على الرغم من حتمية تراكُم نقاط ضعْف الحواسيب الكمومية ونقاط ضعْف الأمن الإلكتروني الحالية، اعتقد الخبراء أن باستطاعة هذا السيناريو أقلّه جعْل وضْعنا آمناً كما هو الآن أو جعْله أكثر أمناً. ومع ذلك، قد يعتمد هذا الأمر بشكل كامل على تحديد الأولويات الحكومية والتجارية المناسبة وإدارة مخاطر التهديد الناتج عن الحواسيب الكمومية. في حال عدم أخذ التهديد على محمل الجد، يُتوقّع أن تكون الولايات المتحدة أقل أمناً في هذا السيناريو عمّا هي عليه اليوم. وقد لخَّص أحد الخبراء الأمر على النحو التالي:

> إذا تعامَل عدد كافٍ منا مع إدارة دورة الحياة، فسيكون لدينا بالفعل أسس تشفير أقوى. ستكون الأمور أفضل قليلاً. إذا ماطل معظم الناس، وانتظروا التهديد حتى يحدق بهم مباشرة، فسيكون الأمر أسوأ ممّا هو عليه اليوم بقليل.

قضيّة متعدّدة الجوانب: التَقِط الآن واستغِل لاحقاً

لقد اقْتَصَرَت مناقشة السيناريوهات إلى حدٍّ كبيرٍ على نقاط الضعف في المصادقة والقضايا التي يجب حلّها مباشرةً قبل

تمّ تقييم السيناريو رقم 3 على أنّه الأقرب إلى وضْع ضعف الأمن الإلكتروني القائم، على الرغم من أنّ معظم الخبراء أشاروا إلى أنّ هذا السيناريو قد لا يزال على الأقل أسوأ من الوضع الحالي بقليل.

استخدام حاسوبٍ كموميّ. وخلال مناقشات هذه السيناريوهات، أشار الخبراء أيضاً إلى قضايا لم تقتصر على سيناريو معيّن واحد ولكن، عوضاً عن ذلك، قد تكون ذات صلة في عدّة سيناريوهات. اعتُبر الخطر الناتج عن المعلومات الملتقطة الآن والتي يتمّ فك تشفيرها بمجرد ابتكار حاسوبٍ كموميّ، على وجه الخصوص، على أنّه نقطة ضعْف موجودة في السيناريوهات الثلاثة جميعها. وأشار الخبراء إلى أنّ المخاطر الناجمة عن هذه القضية كانت قائمة أصلاً لدى عدّة منظمات، وفي النهاية، سيسوء الوضع كلّما أصْبَحَت الفجوة أقصر بين وقت تطبيق التشفير ما بعد الكمّ (PQC) ووقت ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير. علاوةً على ذلك، أعرَبَ الخبراء عن قدرٍ كبيرٍ من عدم اليقين بشأن درجة الخطر، ذلك لأنّ الخطر قد يختلف اختلافاً كبيراً بين منظمة وأخرى بحسب أصولها الحسّاسة الخاصة واستخدامها التشفير، ولأنه من غير المؤكد كيف قد يتمّ في نهاية المطاف استخدام المعلومات الملتقطة لإلحاق الضرر بها. قال أحد الخبراء، "لا أعرف بالضبط كيف سيستغلّ المجرمون الإلكترونيّون والجهات الفاعلة المختلفة هذه المعلومات ويكسبون المال منها أو يؤذون الناس أو يدفعون بأغراضهم السياسية قُدُماً، لأنها تأسيسيّة وجديدة." في حين قلَّل بعض مَن أُجريت معهم المقابلات من أهمية هذه القضية في السيناريوهات اللاحقة، حيث تكون قد مرَّت أعوام متعدّدة على أي اتّصالات بتاريخ فكّ تشفيرها وقراءتها، اقترح عددٌ آخر منهم أنّ الخطر لم يكن كبيراً فحسب، بل قد نتعامل مع آثاره لأعوامٍ أو عقودٍ قادمة. وبغض النظر عن حالات عدم اليقين، اعتبروا بشكلٍ عام أنّ الحدّ من المخاطر تَطَلَّبَ تطبيق التشفير ما بعد الكمّ في أسرع وقت ممكن، ورأوا أنّه يجب على المنظمات الفردية إجراء تقييمات للمخاطر لقياس الخطر التنظيمي الذي واجَهَته، بناءً على الجداول الزمنية المحتملة لتطوير الحوسبة الكمومية، والمعلومات الحسّاسة التي تمّ ضمان أمنها بواسطة التشفير باستخدام المفتاح العام (PKC)، والاستخدام التنظيمي العام للبنية التحتية للمفاتيح العامّة (PKI)، وتحديد هوية الجهات الفاعلة المُهَدِّدة المحتملة.

"إذا تعامَل عدد كافٍ منا مع إدارة دورة الحياة، فسيكون لدينا بالفعل أسس تشفير أقوى."

العوامل التخفيفية

تجدر الإشارة إلى أنّنا طلبنا من الخبراء تقييم مستوى الخطر أو الضعف لكلّ سيناريو مفترضين أنّه لم يتمّ اتخاذ أي إجراءات مضادة إضافية سوى تطبيق التشفير ما بعد الكمّ (PQC) بشكلٍ ملائم. ولكن، أشار الخبراء أيضاً إلى عدد من العوامل التخفيفية التي قد تحُدّ من الضعف الحقيقي الذي يمكن مواجهته، في حال امتلاك جهة فاعلة مهدِّدة حاسوباً كمومياً.

لقد تحدَّثَ عدد من الخبراء عن المحدوديات الواقعية التي يجب توقُّعها من حاسوبٍ كموميٍّ ذي قدرة ناشئة مرتبطة بمشاكل التشفير. في البداية، من المرجح أن تكون هذه المشاكل محفوفة بالتحديات حتى بالنسبة لخصوم يمتلكون موارد كبيرة لأنّها تتطلّب فِرقاً متخصصة من الخبراء للتشغيل. ومن المُرَجَّح أيضاً أن تكون هذه التطبيقات كثيفة الموارد من الناحية الحسابية، واعتَقَد الخبراء أنّه أقله في البداية، قد يستغرق حلّ أيّ مشكلة ذات صلة بالتشفير، مثل اختراق زوج مفتاحين عام–خاص قوي، أسابيع أو أشهُر. في ظلّ تلك الظروف، قد يحتاج أيّ خصم يمتلك حاسوباً كموميّاً ذا صلة بالتشفير إلى تحديد أولويات الأهداف بدقة، مع السعي وراء عدد قليل من الأهداف الأعلى قيمة فحسب على مدى أشهُر أو أعوام بعد استخدام الجهاز لأوّل مرّة. ومع تحسُّن التكنولوجيا وتقليص القيود، قد تتوسّع قائمة الأهداف أو الأهداف المحتملة، ولكن ربما تكون هناك مرحلة تبقى فيها القدرة محدودة حتى ولو أصبح وجودها معروفاً أو مُشتبهاً به بشكل متزايد على نطاق واسع، ممّا يوفّر الفرصة والدافع على حدٍّ سواء لغالبية المنظمات للانتقال إلى التشفير ما بعد الكمّ.

قد يؤثر فرْز الأهداف الناجم عن قيود الموارد أيضاً بشكل غير متناسب على نقاط الضعف الناتجة عن الاتصالات السابقة بانتظار فك تشفيرها بواسطة حاسوبٍ كموميّ. وأشار أحد الخبراء إلى أنّه في حال كان الخصم يلتقط حركة مشفرة، قد يكون عددها كبير بانتظار فكّ تشفيرها. بالإضافة إلى ذلك، قد يكون من الصعب للغاية التمييز بين الاتصالات التي من المرجح أن تكون ذات قيمة وتلك التي لا تهمّ في حركة الاتصالات المشفرة المختلطة. أخيراً، غالباً ما يتمّ توليد مفاتيح عامّة مؤقّتة جديدة لحماية جلسات اتصال جديدة، ممّا قد يترك كميّة صغيرة فقط من المعلومات القيّمة التي يمكن اكتشافها جراء اختراق أي مفتاح.[15] ما لم يكن لدى خصم طريقة ما لمعرفة أنّ اختراق المفتاح العام الذي يحمي تدفّقاً معيناً من الاتصالات سينتج عنه معلومات قيّمة، من الأكثر ترجيحاً أن يسعى وراء أهداف أخرى أكثر فائدةٍ بشكل واضح في البداية، أقلّه حتى تصبح التكنولوجيا أكثر فعاليةً في مهاجمة مشاكل التشفير. بالنسبة إلى عدّة منظمات، قد يحدّ هذا الأمر من الخطر الناجم عن

نقاط الضعف بشكل كبير، حيث سيُسمح للمعلومات المُلتقطة من أهداف أقل قيمةً بالتواري والبقاء غير مقروءة لفترة طويلة تتخطى الفترة التي تكون خلالها مفيدة.

بمجرد أن أصبح أوّل هجوم مُمكَّن بواسطة حاسوب كمومي معروفاً، وربما بمجرد الاشتباه بوجوده، قد تبدأ منظمات متعدّدة لم تطبّق بعد التشفير ما بعد الكمّ باتّخاذ إجراءات وقائية قصيرة الأجل لحماية نفسها. وقد تَضَع المنظمات سياسات وضوابط للتخفيف من الخطر بدرجة معيّنة بينما يتمّ تطبيق الحل الطويل الأجل وهو تطبيق التشفير ما بعد الكمّ. على سبيل المثال، قد تقوم هيئة إصدار شهادات (CA) بتبديل مفتاحها العام على نطاقات زمنية أقصر أي أسابيع، بدلاً من أشهُر، أو يمكن وضْع أنظمة شهادة أكثر شفافية لتحديد الهجمات (إنْ لم يكن لمنْعها).[16] ومع تحسُّن قدرات الحوسبة الكمومية، قد تثبُت عدم كفاية هذا الأمر في النهاية ضدّ خصم مخصص مع حاسوب كمومي، ولكنه قد يجعل المنظمة هدفاً أكثر صعوبةً ويحدّ من الخطر أثناء انتقالها إلى التشفير ما بعد الكمّ. يمكن للمنظمات أيضاً تقليص مساحة هجومها من خلال خفض استخدام التشفير باستخدام المفتاح العام أو تقييد نقل البيانات المشفّرة إلى الشبكات الموثوقة مؤقتاً. في الحالات القصوى، يمكن التبديل في استخدام أساليب توزيع المفاتيح، فيمكن مثلاً استخدام مخططات توزيع المفاتيح المتناظرة مع شركات البريد الموثوق بها. سيقترن أي من هذه التدابير، من الأخفّ إلى الأكثر شدّة، بتكاليف الفعالية على الوضع القائم، لكنها قد تساهم في التخفيف من الخطر مؤقتاً وبشكل فعّال بينما تنتقل المنظمات إلى حل أطول أجلاً.

الأفكار المُسْتَنْتَجة الرئيسية: يُعتَبَر الزمن جوهرياً عند تطبيق التشفير ما بعد الكمّ (PQC) لتبادل المفاتيح في الاتصالات. من المهمّ جدّاً أن يكون التشفير ما بعد الكمّ للمصادقة والمخاطر الأخرى الناجمة عن فك التشفير "الآني" قد طُبِّق عندما تصبح الحواسيب الكمومية تهديداً محقَقّاً، ولكن، باستثناء حدوث قفزات تكنولوجية كبيرة في السرّ، فمن المرجح أن تُطبِّق معظم الأنظمة ذلك في الوقت المناسب. ومع ذلك، فإن الخطر الناجم عن الاتصالات التي يمكن التقاطها الآن وفك تشفيرها لاحقاً، قائمٌ أصلاً وسينمو كلّما تأخَّرَ الانتقال إلى التشفير ما بعد الكمّ في تبادُل المفاتيح. يجب أن يكون بعض المنظّمات الاستثنائية قد بدأ أصلاً بالتفكير في تطبيق التشفير ما بعد الكمّ، حتى قبل أن يصبح معيارٌ جاهزاً، بسبب المعلومات العالية الحساسية التي يحتفظ بها، في حين يجب أن تتخذ غالبية المنظمات أقلّه خطوات تحضيرية للانتقال، مثل جرْد استخدامها للبنية التحتية للمفاتيح العامة (PKI) وتقييم الخطر التنظيمي. قد تواجه المنظمات التي قلّما تستخدِم البنية التحتية للمفاتيح العامة والتشفير باستخدام المفتاح العام (PKC) خطراً ضئيلاً ويمكنها بالتالي الانتظار، بينما قد تحتاج المنظمات الأخرى التي تنقل معلومات حساسة بشكل مكثّف باستخدام هذه الأساليب إلى التصرف في أسرع وقت ممكن. ويتوجب على كلّ منظمة تقييم الخطر التنظيمي الناتج عن الحواسيب الكمومية اليوم، مع مراعاة مساحة الهجوم، وحساسية المعلومات التي تمُسّ بنية تحتية للمفاتيح العامّة، والوقت الذي يجب أن تبقى فيه هذه المعلومات آمنة، وتحديد هويّة الجهات الفاعلة المُهدِّدة المُتوقّعة.

تداعيات الجدول الزمني لابتكار حاسوبٍ كموميّ

لقد أشار الخبراء في المتوسّط إلى أنّ العام 2033 هو التاريخ الأكثر ترجيحاً لابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير، وهذا يتّسق مع التقديرات الأخرى في الدراسات السابقة. يُعتبر جدول التطوير الزمني الممتدّ على فترة 15 عاماً بعيداً بما يكفي للاعتراف بالعقبات العلمية والهندسية الهامة، المعروفة وغير المعروفة منها، والتي ما زال يجب التغلب عليها. في الوقت عينه، إنّه قريب بما يكفي بحيث لا يمكن بسهولة تجاهُل التداعيات الأمنية المترتبة على ابتكاره، لا سيما بالنظر إلى الإجراءات التحضيرية التي قد تستغرق مُهَلاً زمنية طويلة جداً.

لا تزال أمورٌ مجهولةٌ متعدّدةٌ قائمةً في خريطة طريق التطوير، ما يجعل التنبؤات صعبة، وينعكس هذا الأمر في المجموعة الكبيرة من الجداول الزمنيّة المُقدَّمة من الخبراء الذين قابلناهم. لقد أشار الخبراء إلى أنّ التوقّعات المتطرّفة لجهة إمكانية الاعتماد المبكر أو المتأخّر في جدول التطوير الزمني ممكنة. فقد اعتُبِرَت الجداول الزمنية للتطوير على المدى القريب جداً ممكنة خلال العقد المقبل، كما يمكن أن يتبيّن في نهاية المطاف أنّ إمكانية تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير مستحيل عمليّاً. قد تكون القفزات المفاجئة وغير المتوقعة في القدرة ممكنة بفضل الاكتشافات العلمية الأساسية الجديدة. يمكن لهذا التقدُّم غير الخطّي في القدرة أن يتضاعف أيضاً من خلال تأثير السباق إلى النهاية في حال اعتُبِرت التكنولوجيا مجدية بشكلٍ وشيك، بمعنى أنّ الكثير من الأموال والجهود تُبذل لاتخاذ خطوات التطوير الأخيرة لإعلان انتصار تاريخي. والعكس ممكن أيضاً؛ فقد يتباطأ الاستثمار البحثي في الحوسبة الكمومية بسبب نقص التقدُّم المتصوَّر.

يخضع تقييم الأمور ذات الصلة بالتشفير للتغيير أيضاً. تستند التقديرات الحالية لمتطلبات موارد الحوسبة الكمومية إلى متغيّرات خوارزمية شور (Shor)، وخلافاً لخوارزميات البحث في قواعد البيانات الكمومية، لم يتمّ إثبات أنّ خوارزمية شور هي الأفضل لتحليل العدد إلى عوامل. يستمرّ البحث في

خوارزميات أكثر فعالية؛ ويُعتبر التحليل الكموميّ المُتغيّر للعدد إلى عوامل أحد الأمثلة على ذلك (آنشوتز وآخرون [Anschuetz et al.]، 2018). تُعتبر الحوسبة الكمومية وتطوير الخوارزميات الكمومية مجالين حديثَيْن نسبياً مقارنةً بنظرية التعقيد الحسابي العامة، وقد يتبيّن فيما بعد أنّ خوارزميات أكثر فعالية ممكنة لمشاكل مثل تحليل العدد إلى عوامل. وفي حال اكتشاف خوارزميات أكثر فعالية، قد تقلّص هذه الخوارزميّات متطلبات الموارد إلى حدٍّ كبير، مما يجعل بالتالي نظام حوسبة كمومية أقلّ قدرة ملائماً لحلّ مشاكل التشفير ويدفع قُدُماً بالجدول الزمني لابتكار حاسوب كمومي ذي صلة بالتشفير.

وفي وجه حالة من هذا القبيل، اقترح عديدون أنّ استجابة إحتمالية لإدارة المخاطر ضرورية (موسكا [Mosca]، 2015). يجب أن تأخذ إدارة المخاطر الناتجة عن التهديدات من الحوسبة الكمومية في عين الاعتبار الجداول الزمنيّة المنخفضة الاحتمال والعالية العواقب في الحالات القصوى، والجداول الزمنية التي تمتدّ لعقود والأكثر ترجيحاً. وبحسب ما لاحظه أحد الذين قابلناهم، "إنّ الأمن قائم على المخاطر نوعاً ما في هذه الأيام، لذا عليك الاستعداد للاحتمالات. فالجهد الذي تبذله يتناسب بشكلٍ أساسيٍّ مع الخطر الذي تتصوّره. ومن منظور الاستثمار الأمني إنّ الأمر غير مهمّ فعلاً. فإن كان للخطر وجود، علينا أن نستعدّ له." قد تتطلّب مقاربة مماثلة لإدارة المخاطر تقييماً للمخاطر من النوع الذي وصفه موسكا ومولهولند (Mosca and Mulholland) (2017)، والمذكور أيضاً في تقرير الأكاديميات الوطنيّة للعلوم (NAS) حول الحوسبة الكمومية (الأكاديميات الوطنيّة للعلوم [NAS]، 2018a). قد يراعي مثل هذا التقييم للمخاطر حتماً نقاط الضعف التنظيميّة الفرديّة في وجه تهديدٍ ناتجٍ عن الحواسيب الكمومية، وإجراء تقييمٍ لتحديد هوية الجهات الفاعلة المهدِّدَة التي تملك القدرة والدافع على حدّ سواء للبحث عن معلومات حساسة باستخدام حاسوب كمومي، ولمعرفة سرعة تطوير حاسوب كمومي ذي صلة بالتشفير. ستدعو الحاجة إلى إعادة تقييم الجدول الزمني لتطوير حاسوب كمومي ذي صلة بالتشفير بشكل دوري مع تحقيق مراحل التطوير الرئيسية، وستبقى استنباطات آراء الخبراء هذه مفيدة في هذا الصدد.

الأفكار المُسْتَنْتَجة الرئيسية: في حين لا تزال التقديرات المرتبطة بتاريخ ظهور حاسوب كمومي ذي صلة بالتشفير تشير إلى أنّه على بُعد "15 عاماً تقريباً"، يشير الخبراء إلى أنّ الإحتمالات المتطرّفة لجهة إمكانية التطوير المبكر أو المتأخر في جدول التطوير الزمني ممكنة على حد سواء. علاوةً على ذلك، ثمة مراحل تكنولوجية رئيسية وتقديرات للموارد معروفة على المدى القريب لما يشكّل أموراً ذات صلة بالتشفير والتي يمكن استخدامها بمثابة علامات لتحديث الجدول الزمني المتوقّع على امتداد العقد المقبل والحد من عدم اليقين بمرور الوقت. يتوجّب على هؤلاء القلقين إزاء ظهور الحوسبة الكمومية، وخاصةً هؤلاء المسؤولين عن إجراءات الحد من الخطر التي قد تستغرق أعواماً أو عقوداً لتطبيقها، إجراء تقييمات للخطر الناتج عن الحوسبة الكمومية والاستمرار بمتابعة هذه العلامات عن كثب لتقليص إمكانية المفاجأة.

تداعيات الجدول الزمني لاعتماد التشفير ما بعد الكمّ (PQC)

انتقالٌ محفوفٌ بالتحديات

لقد أشار الخبراء إلى فترات عمليات الانتقال إلى التشفير السابقة والتحديات المرتبطة بها لتبرير توقعاتهم حول جداول الاعتماد الزمنية. يقدّم تقرير الأكاديميات الوطنيّة للعلوم (NAS) الأخير حول الحوسبة الكمومية أيضاً تفاصيل حول الخطوات والتحديات المتعدّدة المرتبطة بالانتقال إلى التشفير ما بعد الكمّ (PQC) والتي قد تطيله على مدار عقود (الأكاديميات الوطنيّة للعلوم [NAS]، 2018b). يشمل مصطلح الانتقال إلى التشفير ما بعد الكمّ عدداً كبيراً من عمليات الانتقال إلى التشفير الواجب تطبيقها على امتداد البنية التحتية الكاملة للاتصالات الشبكية، في كل حالة مرتبطة ببنيةٍ تحتية للمفاتيح العامّة (PKI)، وسيتضمن عدداً من عمليات الانتقال الهامة المشابهة أو الأكثر توسعاً في النطاق مقارنةً بهذه الأمثلة التاريخية. على سبيل المثال، بمجرد إصدار معيارٍ للتشفير ما بعد الكمّ، ستحتاج البروتوكولات مثل أمان طبقة النقل (TLS) إلى دْمج تلك الخوارزميات. لقد اقترح أحد الخبراء أنّ دمْج التشفير ما بعد الكمّ في بروتوكولٍ جديدٍ لأمان طبقة النقل قد يتطلّب ثلاثة أعوام في إطار تفاؤلي. ومن المرجح أن تعتمد معظم المنظمات بروتوكول أمان طبقة النقل الجديد في غضون بضعة أعوام، ولكن ستدعو الحاجة إلى اعتماد هذا البروتوكول عموماً تقريباً قبل أن يتمّ التخلّي عن البروتوكولات الضعيفة السابقة. سيستغرق أمان طبقة النقل – النسخة 1.0 ما يقارب 20 عاماً قبل أن يتمّ التخلّي عنه نهائياً، لذلك، ومن الناحية الواقعية، إذا أُصدر معيارٌ للتشفير ما بعد الكمّ بحلول العام 2023، كما هو متوقَّع، من المرجّح أن تبقى تطبيقات أمان طبقة النقل الضعيفة قيد الاستخدام في منتصف ثلاثينيات القرن الواحد والعشرين. وأشار أحد الخبراء إلى مدى صعوبة القضاء على نقاط الضعف الناتجة عن المعايير القديمة:

> "بصراحة تامة، سيكون هناك دائماً بعض المعدات القديمة التي لا يتذكرها أحد، والتي ستظل تستخدِم

المعيار القديم. لم نتوصّل إلا قبل بضعة أعوام فقط إلى التخلّص من شهادات مستخلص الرسالة – النسخة 5 (MD–5) على الرغم من أنّ عدداً منها قد يكون معطّلاً... ربّما لمدة 15 عاماً تقريباً. ... فيستغرق التخلّي عن هذه المعايير الأقدم وقتاً طويلاً."

يحكم أمان طبقة النقل أمن بعض أنواع الاتصالات الشبكيّة فحسب، ومع ذلك، ستحتاج بروتوكولات أخرى متعدّدة من مجموعة البروتوكولات، مثل تلك التي تحكم شبكات بروتوكول الإنترنت والشبكات الخاصة الافتراضية، أيضاً إلى انتقالٍ مماثل إلى التشفير ما بعد الكمّ.

في حين لن تُفهم متطلبات المعيار الجديد بالكامل إلّا بعد إصداره، اعتَقَد الخبراء أنّه كان هناك سببٌ يدعو إلى الشك في أنّ بعض التغييرات قد يجعل عمليات الانتقال محفوفة بالتحديات بشكل خاص. قد تكون الافتراضات الملازمة في البرمجيات والمعَدّات الحاسوبية مثل أطوال المفاتيح المفترضة أو أحجام التواقيع الرقمية، غير متوافقة مع معيار التشفير ما بعد الكمّ، ممّا يجعل الأنظمة غير قادرة على التعامل مع التشفير ما بعد الكمّ على أنّه بديل مطابق. سيكون من الممكن تكييف عدد من هذه الافتراضات بسهولة إلى حدٍّ ما لاستيعاب معيار التشفير ما بعد الكمّ، وخاصة عندما يتعلّق الأمر بتغييرات بسيطة فقط في البرمجيات، ولكن أُعطِي عدد من الأمثلة على مشاكل أكثر استعصاءً قد تتم مواجهتها. وشملت هذه الأمثلة أموراً مثل رمز مصادقة التوقيع الذي لا يمكن ترقيعه (تصحيحه) في المعالِجات، وهيكليات البيانات المضمنة في كل ملف قابل للتنفيذ في نظام التشغيل والتي لا تحتمل طول مفتاح التشفير ما بعد الكمّ، وأجزاء في وحدات المنصات النمطيّة الموثوقة أو نماذج وحدات أمن المعَدّات الحاسوبية النمطيّة التي لا تتمتع بالمرونة للتعامل مع مخططات تشفير أخرى. وقال أحد الخبراء:

> أخشى وجود افتراضات ملازمة في حُزَم البرمجيات في جميع أنحاء العالَم والتي تقول إنّ طول المفاتيح العامة لا يزيد أبداً عن 4,096 بتة (bits)، لأن هذا هو مفتاح خوارزميّة RSA العمليّ الأكبر الذي يستخدمه أي شخص. ... ولكن ماذا يحدث عندما تستخدِم مخطط ما بعد الكمّ لمفتاح عام قائم على الشبكية حيث تكون أطوال المفاتيح من 9 إلى 10 كيلوبايت، وتخترق فجأةً قواعد البيانات، وتخترق البرمجيات، وتوجِّب ترقيع (تصحيح) البرمجيات؟ لا تُعتبر بالضرورة بدائل مطابقة.

قد تتطلب هذه المشاكل أعواماً لتطوير معدّات حاسوبيّة وبرمجيّات جديدة والحصول عليها قبل إمكانية البدء بالتطبيق على نطاق واسع، وحتى بالنسبة إلى أولئك الذين يرغبون في دفْع تكاليف الانتقال الباهظة.

"بصراحة تامة، سيكون هناك دائماً بعض المعدات القديمة التي لا يتذكرها أحد، والتي ستظل تستخدِم المعيار القديم."

وأخيراً، أشار بعض الخبراء، على وجه الخصوص، إلى تحدّيات التطبيق بعد تطوير المعايير والعقبات المحتملة نتيجة المقتضيات الأكثر تطلّباً. غالباً ما تخضع البروتوكولات والخوارزميات الجديدة لاختبارات تمتدّ على مدار أعوام، لا بل عقود، للكشف عن نقاط الضعف قبل أن يتمّ الوثوق بأنّها آمنة. وبسبب عدم نضوج بروتوكولات التشفير ما بعد الكمّ، اعتَقَد عددٌ من الخبراء أنّ الانتقال إلى التشفير ما بعد الكمّ يجب أن يمُرّ بمرحلتين: مرحلة أولية، تمّ فيها تطبيق مخططات الأمن الهجينة التي تستخدم كلّا من البروتوكولات التقليدية الموثوقة وبروتوكولات التشفير ما بعد الكمّ، يليها الانتقال النهائي إلى التشفير ما بعد الكمّ بمجرد قبول أمن البروتوكول في وجه التهديدات التقليدية. وذكر أحد الخبراء: "لن أشعُر بارتياح للمخاطرة ببنيتنا التحتية وبيانات زبائننا في ظلّ المقاومة الكلاسيكيّة لهذه المخططات ما بعد الكمّ". علاوةً على ذلك، أشار عدد من الخبراء إلى عدد التطبيقات الهائل التي سيتوجب تحديثها. وأشار البعض إلى هذا الأمر بشكلٍ عام، قائلاً إنّه "يجب تضمين [المعايير] في تطبيقاتك المصرفية. يجب أن يكون لمتصفح الانترنت الخاص بك مكتبة تشفير خاصة به تحتمل كلّ شيء بعد الكمّ. يجب أن تكون في تطبيقات هاتفك النقال، وتطبيقات الدردشة. لذا، قد أقلق بشأن الجزء المتعلّق بتطبيق المعايير." بينما ركّز آخرون بشكلٍ أكثر تحديداً على التحديات المتعلّقة بتتبُّع تطبيقات مؤسسةٍ كبيرةٍ أو مكوّناتها، خاصةً عند إقامة شراكات مع عدّة موردين وأطراف ثالثة: "يكمُن التحدي بالنسبة إلينا في إجراء جردةٍ شاملةٍ جداً لمعرفة أين نستخدِم البنية التحتية للمفاتيح العامّة. إننا نُشغِّل 2,600 تطبيق. ترتبط هذه التطبيقات البعض منها بالبعض الآخر وبأطراف ثالثة. أعتقِد أنّ شركات من هذا الحجم تعاني جميعها نوعاً ما للاحتفاظ بجردة جيّدة جدّاً لما يتمّ تشغيله وأين يتم تشغيله." لقد بَرَزَت الحاجة إلى التأكّد من أنّ كلّ عقدةٍ في سلسلة الإمداد أو بنية الاتصالات

والمعالجة التحتية تُطبِّق التشفير ما بعد الكمّ عدّة مرات. قال أحد الخبراء، "عليك أن تُمكِّن التشفير المقاوم للكمّ في سلاسل الإمداد الكاملة قبل أن يتمكّن العميل النهائي من استخدامه فعلاً." لا يكفي أن تُطبِّق التشفير ما بعد الكمّ في منتجاتك الخاصة إن كنت تشتري من موردي المكونات أو تقيم شراكات مع أطراف ثالثة لا تُطبِّقه. قد يؤدي الفشل في طلب تطبيق التشفير ما بعد الكمّ بسرعة لدى الشركاء وخاصة في حالة المنتجات الطويلة الأجل التي تحتوي على مكونات متعدّدة وتنطوي على دورات تصميم وتطوير طويلة، إلى تضمين نقاط ضعْف أمنية في المنتجات المتوفِّرة لعقود قادمة.

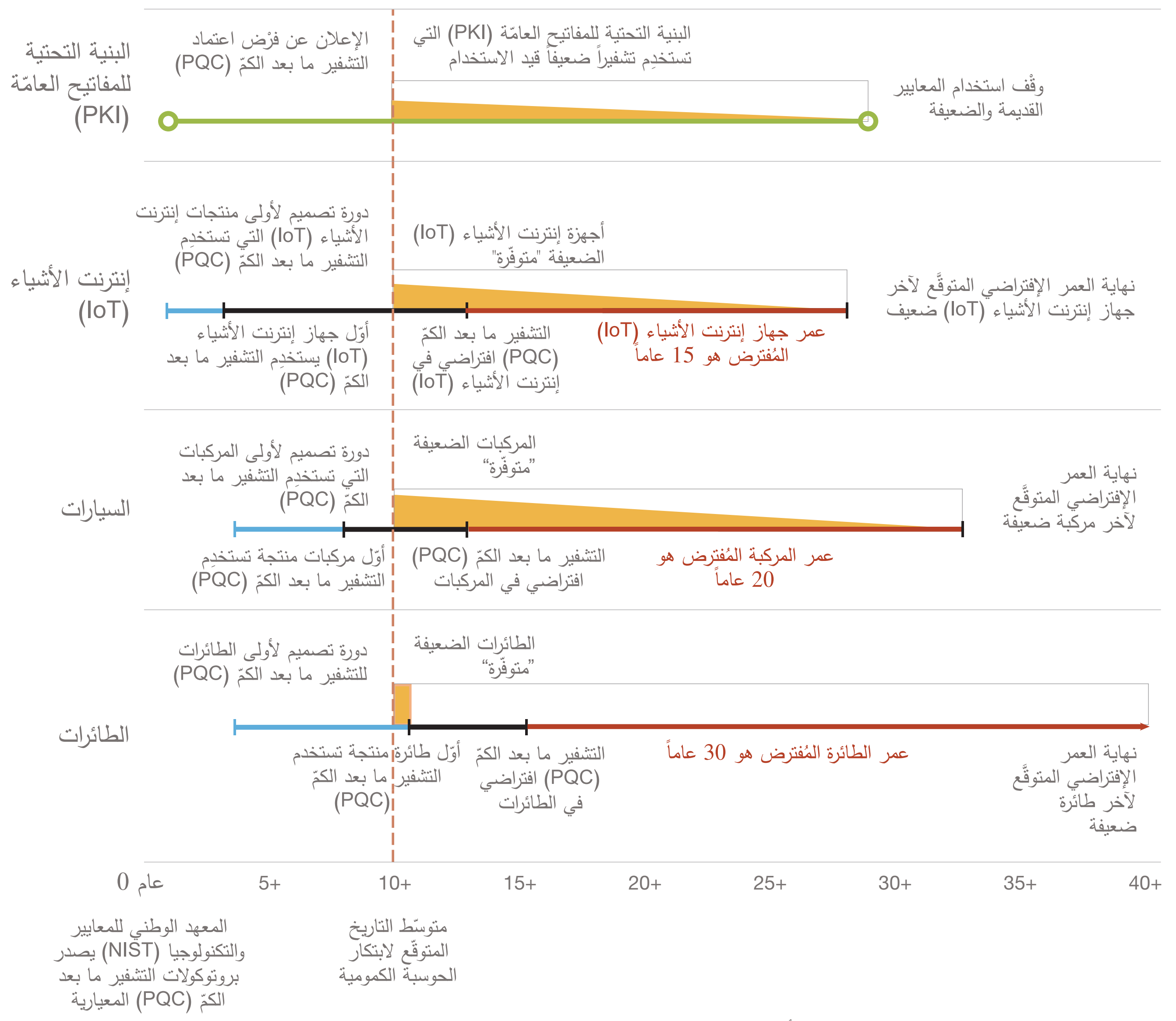
يعرض الشكل رقم 1 الجداول الزمنية الافتراضية التي توضّح كيف ستوسِّع المنتجات الطويلة الأجل والتي تنطوي على دورات تطوير مُطوَّلَة نقاط الضعف في الحواسيب الكمومية في المستقبل البعيد.[17] يوضح الشكل النسبة المئوية النسبيّة للمنتجات "المتوفِّرة" التي ستستند إلى تشفير ضعيف بعد ابتكار حاسوبٍ كموميّ. بالاستناد إلى استنباط آراء الخبراء، نستخدِم التاريخ المتوقّع المتوسط لابتكار حاسوب كمومي ذي صلة بالتشفير ليكون معياراً للمقارنة المرجعية لبداية نقاط الضعف في هذه الأنظمة ونستخدم إصدار المعهد الوطني للمعايير والتكنولوجيا (NIST) لمسودة معيار التشفير ما بعد الكمّ في المستقبل باعتبارها النقطة المرجعية. من المفترض أن يبدأ تطوير معايير بروتوكول جديدة مثل أمان طبقة النقل الذي يشمل خوارزميات التشفير ما بعد الكمّ، وتطوير معدّات حاسوبيّة جديدة مثل وحدات أمن المعدّات الحاسوبيّة النمطية التي تسهّل تطبيق التشفير ما بعد الكمّ، بعد إصدار معيار التشفير ما بعد الكمّ بوقت قصير، واعتَقَد الخبراء أنّ البروتوكولات المعياريّة الجديدة قد تكون جاهزة في غضون ثلاثة أعوام تقريباً. بعد ذلك، يُفترض أن تعتمِد منظمات عديدة التشفير ما بعد الكمّ في البنية التحتية للمفاتيح العامّة بسرعة، على الرغم من الذيل الطويل المُمتدّ على فترة 25 عاماً من تاريخ إصدار معيار جديد. ونتيجةً لذلك، عندما يتم ابتكار الحواسيب الكمومية، ستكون معظم حالات البنية التحتية للمفاتيح العامّة قد انتقلت إلى التشفير ما بعد الكمّ. تُستخدم أجهزة إنترنت الأشياء (Internet of things [IoT]) والسيارات والطائرات على أنّها أمثلة صوَريّة لبعض المنتجات الطويلة الأجل. سيكون لكلّ منها فترات مختلفة لمتوسط دورات تطوير المنتج وعمر المنتج. وغالباً ما تتطلّب تعديلات الأنظمة القائمة على البرمجيات المطابقة في المركبات عاميْن على الأقل من التطوير والاختبار، وقد يكون دمْج التشفير ما بعد الكمّ في أمن المركبات أكثر تعقيداً (بورجس [Porges]، 2015). على وجه الخصوص، من المرجح أن تكون أعمال تطوير منتجات نظم الأنظمة مثل السيارات والطائرات كبيرة وتمتدّ على مدى أعوام عدّة لدمج التشفير ما بعد الكمّ، وخاصة عندما سيتطلّب هذا العمل تصميم معدّات حاسوبية جديدة وإنتاجها، مثل وحدة أمن معدّات المركبات الحاسوبية النمطيّة المتخصّصة الضرورية لحماية وحدات التحكم الإلكترونية داخل المركبة والاتصالات (ولف وجيندروليس [Wolf and Gendrullis]، 2011). تكون نتيجة هذه العوامل ابتكار منتجات ستبقى متوفِّرة لعقودٍ ويكون أمنها ضعيفاً في وجه الحواسيب الكمومية. في حين يمكن تنفيذ البرامج المكلفة لسحب الأنظمة الضعيفة أو تعديلها، يفترض الشكل، على عكس ذلك، أنّ أكثر السيناريوهات احتمالاً هو السيناريو الذي يتمّ فيه استبدال الأنظمة تدريجياً بمنتجات تستخدِم التشفير ما بعد الكمّ بمجرد انتهاء عمرها الافتراضي. يهدف هذا الشكل الصوري إلى تسليط الضوء على أهمية إعطاء الأولوية لاعتماد التشفير ما بعد الكمّ للحد من نطاق الضعف في وجه الحواسيب الكمومية، وخاصةً في الصناعات أو المنتجات التي تتمتّع بدورات تطوير أو أعمار مُطوَّلَة.[18]

العوامل المؤثّرة على الاعتماد

نظراً إلى التحديات المتوقَّعة مع الانتقال القادم إلى التشفير، ناقشنا أيضاً العوامل التي يمكن أن تؤثِّر على معدّل الاعتماد. لقد ناقشنا العوامِل التي يمكن أن تبطئ أو تسَرِّع معدلات الاعتماد وطلبنا من الخبراء تقديم اقتراحات حول طرق تحفيز اعتمادٍ أسرع وأكثر قوةً للتشفير ما بعد الكمّ (PQC). أشار بعض الخبراء إلى أهمية تصحيح جوانب معينة من عملية توحيد المعايير. وأعربوا عن قلقهم إزاء إصدار عددٍ كبيرٍ من البروتوكولات المقبولة في معيار التشفير ما بعد الكمّ الأمر الذي قد يتسبب بتحديّات في مجال قابلية التشغيل المتبادل ونقاط ضعْف نتيجةً لمزيدٍ من التعقيد. وبشكلٍ مترابط، اعتقدوا أنّه في حال لم يتّبِع المجتمع الدولي الخطوات ذاتها فيما خصّ معيار التشفير ما بعد الكمّ، ستظهَر مشاكل وتحديات إضافية لقابلية التشغيل المتبادل في الصناعة ممّا قد يُبطئ الاعتماد. وأشار عدد من الخبراء أيضاً إلى أنّ اللوائح وإجراءات الفرض غير الملائمة أو الافتقار إلى إجراءات الإنفاذ والامتثال الفعّالة والمتّسقة قد تؤدي على الأرجح إلى اعتمادٍ أبطأ. وأعرَب خبراء آخرون عن قلقهم بشأن تأثير المعيار الجديد على عوامل مثل وقت معالجة المعاملات المالية. كانت السرعة الإجمالية للمعالجة تُعتبر مقياساً رئيسيّاً للأداء، خاصة بالنسبة إلى المؤسسات المالية الكبرى ومعالِجات الدفع، وبالتالي قَلَّ احتمال اعتماد أي حلٍّ يزيد من وقت المعالجة بسرعة. لقد شدّد أحد الخبراء على أنّ "كلّ ثانية مهمّة، ومهما كان الحل، يجب ألا يتسبب بالتأخير، وإلّا لن يعتمده الناس."

الشكل رقم 1

الجدول الزمني الصوَري لنقاط الضعف في المنتجات والأنظمة الطويلة الأجل



ملاحظة: IoT = Internet of Things = إنترنت الأشياء

وقد أشارَت الأبحاث الحديثة حول اعتماد معيار التشفير المتقدّم (AES) إلى أنّ تصوُّر الصناعة لارتفاع تكاليف التحوّل كان عاملاً مهمّاً في تأخير الاعتماد في ذلك الانتقال (ليش، فيريس، وسكوت [Leech, Ferris, and Scott]، 2018)، وردّد عدد من الخبراء الذين قابلناهم هذا القلق بشأن ارتفاع تكاليف الانتقال بالنسبة إلى البنية التحتية وأنظمة الأمن في الانتقال إلى التشفير ما بعد الكمّ. وبشكلٍ خاص، إذا كان الانتقال ينطوي على تطوير معدّات حاسوبيّةٍ جديدةٍ ضروريّةٍ للحدّ من التحدّيات الناجمة عن التعقيد المتزايد، ومقتضيات التشفير المتطلِّبة، وزيادة أوقات المعالجة وعلى امتلاك هذه المعدّات، اعتبَر الخبراء أنّ تكاليف الانتقال قد تكون مرتفعة. وأخيراً، ظنّ الخبراء أنّه قد يتمّ الافتقار إلى حِسّ الاستعجال الجَماعي للحدّ من التهديد، خاصةً إذا استمرّ التصوُّر بأنّ الحواسيب الكمومية ذات الصلة بالتشفير هي على بُعد عقود ولم يُتَصَوَّر أي تهديد على المدى القريب. واعتبَر الخبراء أنّ تصوّرات تكاليف الانتقال المرتفعة مضافةً إلى الافتقار إلى حِسّ الاستعجال الجَماعي في بعض القطاعات، قد يؤديان إلى تباطؤ منظمات متعددة

لقد شدّد أحد الخبراء على أنّ "كلّ ثانية مهِمّة، ومهما كان الحل، يجب ألا يتسبب بالتأخير، وإلّا لن يعتمده الناس."

في الاعتماد، في حين تَعْمَد منظّمات متعدّدة إلى الاعتماد "الضمني" فحسب. وقد عَنَوا بذلك أنّ المنظمات قد لا تتخذ أي تدبيرٍ محدّدٍ للاعتماد. فهي قد تستبدل الأنظمة الحالية في التكنولوجيا المتهالكة ودورات الاستبدال العاديّة، بحيث قد لا يحدث التحوّل إلى التشفير ما بعد الكمّ بحكم الواقع إلّا عندما تَستَخدم جميع أنظمة الاستبدال في السوق التشفير ما بعد الكمّ على أنّه ضمني. "من الأكثر ترجيحاً ألّا تستبدل في الواقع تكنولوجيتها الحالية وألّا تُحَدِّثها، بل أن تشتري منتجات جديدة لأنّ المنتجات القديمة ... لم تَعُد صالحة أو توقَّفت عن العمل. وبالتالي ستنتج عن ذلك ... فترةٌ زمنيّةٌ طويلةٌ تُستبدل خلالها المنتجات بالقِطَع."

لقد أشار الخبراء الذين قابلناهم أيضاً إلى عوامل قد تساعد على تسريع الاعتماد. وكان أحد أكثر هذه الآراء شيوعاً التصوّر السائد على نطاقٍ واسع بأنّ التهديد الناجم عن الحوسبة الكمومية وشيك. وفي حين غالباً ما أشار الخبراء إلى الحاجة إلى توقّعات واقعية للتهديد وتجنُّب إثارة الخوف، اقترحوا أنّ مساعدة المنظمات على فهْم الضعْف الحقيقي الذي تواجهه الآن وفي المستقبل القريب قد يساهم في تسريع اعتماد التشفير ما بعد الكمّ بمجرد إصدار معيار. بالتزامن مع ذلك، أشار البعض إلى أنّ اللوائح الفعالة وإجراءات الفرض والإنفاذ والتحفيز قد تزيد من سرعة الاعتماد. وأشاروا إلى أنّ مزاعم الملكية الفكرية على بروتوكولات التشفير قد أعاقت في الماضي اعتماد تكنولوجيات واعدة وكانوا يأملون أن يفضّل نشاط المعهد الوطني للمعايير والتكنولوجيا (NIST) لتوحيد معيار التشفير ما بعد الكمّ بشكلٍ صريحٍ الخوارزميات التي التزَم مالكوها بمَنحِها التراخيص من دون مقابل (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2017). كان من المتوقّع أيضاً ملاحظة زيادة قوية ومتعاقبة في الاعتماد إذا ما قام عدد قليل من الجهات الفاعلة الرئيسية في مختلف الصناعات بالاعتماد باكراً، حيث تَلْتَهم شركات أخرى بسبب الضغط التنافسي. على وجه الخصوص، إذا قام بعض المؤسسات المالية الكبيرة أو مقاولي الدفاع بالاعتماد، توقَّع الخبراء أن يتسبّب ذلك بنوعٍ من "المرحلة الانتقالية" في صناعاتهم، قد تليهم فيها مؤسسات أخرى متعدّدة. وقال أحدهم، "لا تحتاج إلى الجميع للقيام بذلك. أنتَ بحاجة فقط إلى ما يكفي من الجهات الفاعلة الرئيسية. ... يمكن للآخرين النَسخ واللصق، لكنك تحتاج إلى عددٍ حاسمٍ من الأشخاص الجادين للقيام بذلك بشكلٍ صحيح." وأشار آخرون أيضاً إلى إمكانية تحفيز اعتمادٍ أفضل للأمن من خلال الاتفاقيات التي تُحمِّل الشركاء مسؤولية الإخفاقات الأمنية إذا فشلوا في اعتماد التشفير ما بعد الكمّ. وأشار الخبراء إلى أمثلة مثل الاتفاقيات المبرمة بين معالِجات الدفع والتجار، حيث أنّ معالِجات الدفع مسؤولة عن المعاملات الاحتيالية، بينما يُحمَّل التجار المسؤولية المالية إذا لم يستخدموا أساليب المصادقة الأكثر أمناً. وقد يؤدّي إيجاد طرق إبداعية مماثلة لتحفيز الشركاء والموردين على اعتماد التشفير ما بعد الكمّ إلى تسريع الاعتماد على نطاقٍ أوسع.

لدى الحكومة الأمريكية منظمات يمكن أن تكون مفيدة في الدفع بالتغيير في بنية الاتصالات وتكنولوجيا المعلومات التحتية الخاصة بنا، ومن المرجح أن تكون التدابير المتَّخَذة من قِبل هذه المنظمات بالغة الأهمية في تحفيز التغييرات المرتبطة باعتماد التشفير ما بعد الكمّ استجابةً للتنسيق المركزي. اضطلع كلّ من المعهد الوطني للمعايير والتكنولوجيا (NIST) (بدعمٍ من وكالة الأمن القومي [NSA])، ووكالة الأمن الإلكتروني وأمن البنية التحتية (Cybersecurity and Infrastructure Security Agency [CISA]) في وزارة الأمن الداخلي والإدارة القومية للاتصالات والمعلومات (National Telecommunications and Information Administration [NTIA])، وإدارة الخدمات العامة (General Services Administration [GSA]) ومكتب الإدارة والموازنة (Office of Management and Budget [OMB]) بأدوار رئيسية في عقْد الإجتماعات أو تمتَّعَت بصلاحيات لوضع المعايير في هذا المجال.

على وجه الخصوص، يضطلع كلّ من المعهد الوطني للمعايير والتكنولوجيا ووكالة الأمن الإلكتروني وأمن البنية التحتية بأدوار أساسية في دعوة أصحاب الشأن في الحكومة وقطاع الصناعة للاجتماع من أجل توفير القيادة وتبادُل المعلومات ومعالجة القضايا الأمنية المتعلّقة بتكنولوجيا المعلومات بشكلٍ تعاوني. وتتولّى وكالة الأمن الإلكتروني وأمن البنية التحتيّة مسؤولية التنسيق بين المنظمات الحكومية ومنظمات القطاع الخاص على نطاقٍ واسعٍ لتوفير الحماية الإلكترونية الشاملة ومرونة البنية التحتيّة وإدارة المخاطر الوطنية (وكالة الأمن الإلكتروني وأمن البنية التحتية [CISA]، غير مؤرَّخ) ومن المرجح أن تكون جهةً

فاعلةً رئيسيةً في أي جهود مبذولة للاستجابة لمخاطر أمن تكنولوجيا المعلومات الناجمة عن الحواسيب الكمومية على المستوى الوطني. بالإضافة إلى دوره في عقْد الاجتماعات، يوفِّر المعهد الوطني للمعايير والتكنولوجيا كميّة كبيرة من الوثائق التي توضح بالتفصيل المعايير والإرشادات لتطبيق أمن المعلومات. إنّ المعايير التي يضعها المعهد الوطني للمعايير والتكنولوجيا هي خاصّة بالحكومة الأمريكية، ولكن غالباً ما يتمّ أيضاً اعتمادها واستخدامها من قِبل القطاع الخاص. يُعتبر إطار عمل المعهد الوطني للمعايير والتكنولوجيا لتحسين أمن البنية التحتية الأساسية *(NIST's Framework for Improving Critical Infrastructure Security)* مثلاً أوّلياً على ذلك، وهو يقدِّم الإرشادات حول التأسيس لأمن إلكتروني جيّد ويشير إلى عدد من المراجع والمنشورات الأخرى الغنية بالمعلومات حول كلّ خطوة في إطار العمل (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2018a). قد تشكِّل تحديثات إطار العمل هذا ومراجِعِه خطوة أساسية في تحويل الأولويات والاستراتيجيات على نطاقٍ واسع نحو حماية بنيتنا التحتية من نقاط الضعف في وجْه الحواسيب الكمومية. وتُشكِّل أيضاً معايير معالجة المعلومات الفيدرالية رقم 3–140 الصادرة عن المعهد الوطني للمعايير والتكنولوجيا (NIST FIPS 140–3) التي تُفصّل المتطلّبات الأمنيّة لوحدات التشفير النمطيّة، وثيقةً أساسيةً تحدِّد المعايير ذات الصلة (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2019). ودعماً لمهمته المتمثّلة في توفير القيمة والادخار في الاقتناء، والتكنولوجيا، والخدمات الأخرى على امتداد الحكومة، تقوم إدارة الخدمات العامة بنشر خطة استراتيجية لتكنولوجيا المعلومات بانتظام. تتضمّن هذه الوثيقة رؤية المنظمة ومهمّتها المتعلقة بتكنولوجيا المعلومات وتُحدِّد الأهداف والأغراض الاستراتيجية في هذا المجال. إنّ أحد هذه الأهداف في أحدث خطة استراتيجية لتكنولوجيا المعلومات هو تعزيز الأمن الإلكتروني من خلال تحسين الوعي وفهْم الامتثال للأمن الإلكتروني والتهديدات والتأثيرات وتعزيز ضوابط الأمن الإلكتروني وأدواته (إدارة الخدمات العامة [GSA]، 2018). وبصفتها هيئة المشتريات المركزية لبنية تكنولوجيا المعلومات التحتية التابعة للحكومة الفيدرالية، قد تؤدّي إدارة الخدمات العامّة دوراً هاماً في الدفْع بالتغيير في وضعية الأمن الإلكتروني والأولويات اللازمة للاستعداد لاعتماد التشفير ما بعد الكمّ إذا ما تمّ توجيهه بشكلٍ ملائم. أخيراً، يضطلع مكتب الإدارة والموازنة بمهمّة تطبيق سياسات الرئيس الأمريكي وإنفاذها على امتداد الحكومة. ويتولّى المكتب عمليات الإدارة الرئيسية، مشرفاً على أداء الوكالات، والمشتريات الفيدرالية، وتكنولوجيا المعلومات، والتي تشمل الشواغل المرتبطة بالخصوصية والأمن. بالإضافة إلى ذلك، إنّه مُكَلَّف بتنسيق التشريعات الفيدرالية الهامّة ومراجعتها بهدف ضمان أن تعكُس تأثيرات الأولويّات الرئاسية (مكتب الإدارة والموازنة [OMB]، 2018). تاريخيّاً، تَضمَّنَت المهام التي تقع ضمن نطاق اختصاص المكتب التدابير ذات الصلة مثل تقديم التوجيه بشأن تنفيذ التشريعات حول تحديث تكنولوجيا المعلومات الحكومية (مولفاني [Mulvaney]، 2018) وتحديد المسؤوليات والصلاحيات الرئيسية لمديري المعلومات (chief information officers [CIOs]) في الوكالة (لو [Lew]، 2011). وعلى وجْه الخصوص، من المرجّح أن يكون مديرو المعلومات مسؤولين عن توجيه التغييرات في أنظمة تكنولوجيا المعلومات الخاصة بالوكالة لاستيعاب عمليات الانتقال إلى التشفير ما بعد الكمّ. ويقود مديرو المعلومات عملية الاستثمار في تكنولوجيا المعلومات وهم مسؤولون عن ضمان أمن المعلومات في أنظمة المعلومات التي تدعم مهمة الوكالة.

في نهاية المطاف، حدّدنا اقتراحات متعدّدة من الخبراء الذين قابلناهم بشأن التدابير التي من المحتمل أن تكون فعالة في تحفيز اعتماد التشفير ما بعد الكمّ بشكلٍ أسرع وأكثر انتشاراً وأكثر قوة.

اتخاذ تدابير لجعل توحيد معايير التشفير ما بعد الكمّ (PQC) قابل للتشغيل المتبادل على نطاق واسع قدر الإمكان. كان الخبراء قلقين من أنّ أي عامِل أعاق قابلية التشغيل المتبادل الواسعة النطاق لمعيار التشفير ما بعد الكمّ قد يؤدي في النهاية إلى إبطاء الاعتماد. وأشاروا إلى أنّ نشاط المعهد الوطني للمعايير والتكنولوجيا (NIST) المستمر لتوحيد المعايير يسمح له باختيار خوارزميات متعدّدة مقبولة في المعيار النهائي. وأعربوا عن قلقهم من أنّ السماح بعددٍ كبيرٍ من الخوارزميات قد يُدخل اختلافاً في التطبيق ما قد يُصَعّب الإئتلاف حول تطبيقٍ مشتركٍ وقابل للتشغيل المتبادل. وفي حين تمّ تفضيل إصدار خوارزمية واحدة للتشفير باستخدام المفتاح العام والتواقيع في المعيار، اعتَقَد الخبراء أنّ الحدّ بشكلٍ عام من عدد الخوارزميات المقبولة قد يكون مفيداً. بمجرد إصدار المعيار، لاحَظ الخبراء أيضاً بروز حاجة إلى متابعة عملية نقْل المعيار إلى المنظمة الدولية لتوحيد المقاييس (ISO) لوضع معيارٍ دولي. وأمِلَ الخبراء أن يؤدي معيار فعّال قابل للتشغيل المتبادل دولياً إلى تعزيز الاعتماد بشكلٍ إضافيّ. وأخيراً، أعرَب الخبراء عن قلقهم بشأن نقص تمويل نشاط توحيد المعايير وأبدوا استمرار التمويل الكافي لإنهاء النشاط بشكلٍ جيّد وفي الوقت المحدّد.

وضْع لوائح وآليات إنفاذ فعّالة لفرض الاعتماد على نطاقٍ واسعٍ وتحفيزه. لقد أشار الخبراء مراراً إلى الحاجة إلى لوائح فعّالة لتعزيز الاعتماد بمجرد إصدار معيار. واقترحوا البدء بوضع لوائح تفرض نشْر التشفير ما بعد الكمّ

(PQC) بشكلٍ سريع في المنظمات الحكومية والبنية التحتية الأساسيّة. واقترحوا أيضاً أن تقود الحكومة الجهد عن طريق المطالبة بجعل التشفير ما بعد الكمّ ضمنيّاً بالنسبة إلى جميع الشركات التي تبيع المعدّات الحاسوبية أو البرمجيات للزبائن الحكوميين، وفي نهاية المطاف طلب استبدال أي منتجات تستخدِم خوارزميات التشفير باستخدام المفتاح العام الحالية. وأشاروا إلى أنّ الاتكال على قوى السوق لدفع المنظمات التجارية إلى الاعتماد قد يؤدي غالباً إلى امتناع الشركات عن الاعتماد إلى حين يتمّ اختراقها، في حين يمكن لانتقال بقيادة الحكومة أن يفرض إجراءات أكثر استباقية. ولكن، سارع الخبراء إلى ملاحظة أنّ هذا قد يتطلّب أيضاً إنفاذاً متّسقاً وفعالاً. واستشهدوا بمثل الانتقال إلى التشفير بالمنحنيات الإهليلجيّة بقيادة الحكومة الذي تمّ وقفه مؤخراً، مشيرين إلى أنّ فرْض استخدام التشفير بالمنحنيات الإهليلجيّة على المنظّمات والشركاء الحكوميين لم يتم إنفاذه بشكلٍ كافٍ على كلّ الأطراف، بما في ذلك شركات البرمجيات، وهيئات إصدار الشهادات (CAs)، ومزوّدي الخدمات السحابية، وكثيراً ما تمّ منْح إعفاءات من توفيره. بالنسبة إلى البنية التحتية الأساسيّة المُنظَّمة أصلاً بشكلٍ صارم، قد تكون المسألة متعلّقة بجعل التشفير ما بعد الكمّ أولوية بالنسبة إلى تلك التي تضمن أصلاً الامتثال للّوائح. وأخيراً، أشار الخبراء إلى الفرق بين فرْض الانتقال وضمان الإنفاذ الملائم وأشاروا إلى الحاجة إلى مزيدٍ من التشريع الذي قد يوفِّر مخطّطاً لإصدار الشهادات لتطبيقات التشفير ما بعد الكمّ. قد يساعد ذلك أيضاً على التصدّي لاحتمال وجود نقاط ضعْف ناجمة عن التعقيد الإضافي بسبب الجهود الموازية الرامية إلى زيادة سرعة التشفير.

يجِب على قطاع الصناعة اتّخاذ خطوات استباقية للاستعداد للانتقال إلى التشفير ما بعد الكمّ (PQC) وتعزيز سرعة التشفير. لقد نشر المعهد الوطني للمعايير والتكنولوجيا (NIST) مؤخراً إطار عمل للأمن الإلكتروني يهدف إلى مساعدة المنظمات في تحديد مخاطر الأمن الإلكتروني وتقييمها وإدارتها، ويجب تضمين الخطر الناجم عن الحواسيب الكمومية في أي أنشطة تنظيمية تطبّق إطار العمل هذا (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2018a). على الأقل، يجب على المنظمات أن تنظر في بذْل جهودٍ لجرد استخدامها الخاص للتشفير باستخدام المفتاح العام (PKC) والذي ستدعو الحاجة إلى نَقْله. بالنسبة إلى المنظمات التي تعتمد على عددٍ كبيرٍ من الشركاء والموردين والأطراف الثالثة الأخرى، يجب أيضاً تقييم استخدامات التشفير باستخدام المفتاح العام التي تجري خارج المنظّمة، لأنه في حال كانت المنتجات والتطبيقات الخاضعة للمراقبة الخارجية ضعيفة، فمن المُرَجَّح أن تكون المنظمة الرئيسية ضعيفةً هي الأخرى. ويولي إطار عمل المعهد الوطني للمعايير والتكنولوجيا اهتماماً خاصاً لإدارة مخاطر سلسلة الإمداد، ويجب أن يأخذ تقييم خطر سلسلة الإمداد في الاعتبار الخطر الكمومي. عندما يتمّ تقييم خطرٍ غير مقبول على الشبكات التي تَسْتَخْدم التشفير باستخدام المفتاح العام، قد تحتاج المنظمات إلى النظر في نقْل بعض الاتصالات أو المعلومات مؤقتاً إلى شبكات موثوقة لا تستخدِم التشفير باستخدام المفتاح العام. يجب على المنظمات التي تتمتّع بسلاسل إمداد واسعة النطاق وشركاء كُثُر وضْع خطة لدفع الشركاء للانتقال أيضاً إلى التشفير ما بعد الكمّ، بمجرد إصدار معيار، وقد تحتاج إلى النظر في اختصار سلسلة الإمداد وابتكار المزيد من المنتجات "داخليّاً" لفترة في حال عدم انتقال الشركاء إلى التشفير ما بعد الكمّ. لقد ناقش عددٌ من الخبراء مراراً الانتقال إلى التشفير ما بعد الكمّ على أنّه فرصة فريدة للتحرك الجَماعي نحو سرعة أكبر في التشفير. وأشاروا إلى أنّ كيفية "استهلاك" التطبيقات للتشفير لم تتغيّر منذ عقود. علاوةً على ذلك، من المرجّح أن ينطوي الانتقال إلى التشفير ما بعد الكمّ على بعض التغييرات النظميّة الكبيرة والمعقَّدة والواسعة النطاق في التطبيقات التشفيرية وبالتالي، سيوفِّر فرصةً لإجراء تغييرات على نطاقٍ أوسع سوف تسهّل عمليات الانتقال المستقبلية. لخّص أحد الخبراء هذا الأمر قائلاً: "تتوفّر لنا الفرصة مع هذا التهديد الكمومي وواقع أنّه يجب على الناس الانتقال إلى التشفير ما بعد الكمّ. وتتوفّر لنا الفرصة للنظر في كيفية اتخاذنا تلك الخطوة باتجاه سرعة التشفير، لأنّ الناس لن يتّخذوا هذه الخطوة من دون أمرٍ مماثلٍ يدفعهم إلى القيام بذلك." إذا كان بإمكان قطاع الصناعة تطوير أنظمة تحتاج فحسب إلى التوافق مع مقاربات سياسات التشفير بحيث تستخدِم التشفير عن طريق استدعاء مكتبات التشفير التي تُلبّي متطلّبات معيّنة ويمكن تبديلها بسرعة أو الخروج منها بحسب الحاجة، فيمكن جعلها محايدة لخوارزميات التشفير ومواصفاته الأساسيّة. نَظَرَت ورشة عمل حديثة للأكاديميات الوطنية (National Academies) حول سرعة التشفير وقابلية التشغيل المتبادل في تفاصيل هذه المقاربات وتوجيهاتها الإضافية. في حين يمكن لأنظمة التشفير الأكثر سرعةً أن تحمل خطراً إضافيّاً بسبب ازدياد التعقيد بشكل عام، ساد الاعتقاد بأنّ التطبيق السليم لأنظمة تشفير أكثر سرعةً أساسيّ في جعْل الأنظمة أكثر مرونةً إلكترونيّاً وفي الاستعداد للحواسيب الكمومية (الأكاديميات الوطنية للعلوم [NAS]، 2018a). كان المعهد الوطني للمعايير والتكنولوجيا يشجع أيضاً التركيز على زيادة السرعة في التشفير التنظيمي في الاتصالات الحديثة المرتبطة بالانتقال القادم إلى التشفير ما بعد الكمّ (تشين وآخرون [Chen et al.]، 2016). مؤخراً، تمّ الدفع باتجاه

إجراء تغييرات نظميّة للتوصل إلى سرعة أفضل في التشفير في أماكن أخرى (أشفورد [Ashford]، 2018)، ولاحَظ الخبراء أنّ التعقيد الجوهري لهذا الانتقال قد يشكّل دافعاً يُحفّز قطاع الصناعة على أن يجري بشكلٍ جَماعيٍّ تغييرات في استخدام التشفير ما بعد الكمّ عموماً تمس الحاجة إليها. ومع ذلك، يجب اتخاذ خطوات مصاحِبة لضمان التطبيق الملائم لمقاربات أكثر سرعة، ما لم يؤدِّ التعقيد الإضافي إلى بروز نقاط ضعْف أخرى.

الأفكار المُستَنْتَجة الرئيسية لصانعي السياسات: مثلما هو الحال بالنسبة إلى تقرير الأكاديميات الوطنية للعلوم (NAS) حول تقدُّم الحوسبة الكمومية (الأكاديميات الوطنية للعلوم [NAS]، 2018b)، نلاحظ وجود هامش أمان ضئيل للبدء بالتحوّل إلى التشفير ما بعد الكمّ (PQC) إن لم يكن معدوماً. ففي السيناريو الأكثر ترجيحاً، من المرجح أن تُظهر بنية اتصالاتنا التحتية خطراً كبيراً ناجماً عن الحوسبة الكمومية، حتى لو بدأت الاستعدادات على الفور، وستتعرض الولايات المتحدة لخطرٍ أكبر كلّما تأخرت في ذلك. من المرجّح أن تكون هناك "مواضع شكوى" في عدد من مراحل عملية اعتماد التشفير ما بعد الكمّ قد تُبطئ العملية. سيكلّف كلّ شيء وقتاً ومالاً، بما في ذلك وضْع المعيار، وتضمين البروتوكولات الجديدة في المعدّات الحاسوبيّة والبرمجيات، واعتماد المعيار الجديد بشكلٍ نشِط، وضمان التطبيق الملائم. في غياب تدابير تفرض هذه الخطوات أو تُحفّزها، من المرجح أن يستغرق الاعتماد عقوداً، ممّا يترك نقاط ضعْف كبيرة على امتداد البنية التحتية الوطنية. تبرز الحاجة إلى سياساتٍ تفرض الاعتماد على الحكومة والزبائن الحكوميين، وتوفّر موازنة ملائمة وتمنح الأولوية لتوحيد المعايير وعمليات الانتقال، وتقدّم حوافز للمنظمات غير الحكومية، وتضع مخطّطاً لإصدار الشهادات لتطبيقٍ ملائم. علاوةً على ذلك، يجب وضْع توجيهات حول تقييم الخطر على الأمن الإلكتروني الناجم عن الحواسيب الكمومية ومعالجته والإشارة إليها في الوثائق التوجيهية الحالية والملائمة مثل إطار عمل المعهد الوطني للمعايير والتكنولوجيا لتحسين أمن البنية التحتية الأساسية (NIST *Framework for Improving Critical Infrastructure Cybersecurity*) (2018a). في نهاية المطاف، من المرجّح أن تدعو الحاجة إلى استجابة فيدراليّة مشابهة لتوصية المجلس الاستشاري لاتصالات الأمن القومي (National Security Telecommunications Advisory Committee [NSTAC]) بشأن مبادرة طموحة وابتكارية للأمن الإلكتروني (Cybersecurity Moonshot Initiative) أو الجهوزية للانتقال إلى العام 2000 (Y2K)، وقد تكون مبادرة مُشكَّلة على غرار توصيات المجلس الاستشاري لاتصالات الأمن القومي أو الدروس المستفادة من الاستجابة للانتقال إلى العام 2000 مفيدة في تنسيق القيادة الفيدرالية في سياق اعتماد التشفير ما بعد الكمّ.

يجِب على قطاع الصناعة اتّخاذ خطوات استباقية للاستعداد للانتقال إلى التشفير ما بعد الكمّ (PQC) وتعزيز سرعة التشفير.

الأفكار المُستَنْتَجة الرئيسية للمنظمات الفردية: يجِب على المنظمات جرْد أين يتمّ استخدام البنية التحتية للمفاتيح العامّة (PKI) داخلياً ومع الموردين والشركاء الآخرين. عند الإمكان، يجِب على المنظمات طلب التشفير ما بعد الكمّ (PQC) في أي تطبيقات أو مكوّنات مستخدَمة. يجِب أن يبدأ العمل التحضيري لفهم متطلّبات الانتقال إلى التشفير ما بعد الكمّ في بنية المنظمات التحتية: القيام بعمليات نشْر اختبارية وإجراؤها على البنية التحتية الداخلية، وتحسين أجهزة الزبائن وفي النهاية وقْف تشغيل أنظمة التشفير الضعيفة السابقة في أقرب وقتٍ ممكن عملياً. وبشكلٍ خاص يجب ملاحظة المجالات التي تستخدم فيها الأطراف الثالثة البنية التحتية للمفاتيح العامّة والنظر في الخيارات لتحفيز اعتماد التشفير ما بعد الكمّ من قِبَل هذه الأطراف الثالثة والمورّدين.

استجابات المستهلِكين والتداعيات

لقد أجرينا أيضاً دراسة استقصائية حول المستهلِكين لأنّ المخاطر التي تعترض التشفير والناجمة عن الحوسبة الكمومية تمتد إلى الاقتصاد العالمي الحديث. فإذا قلَّلَ المستهلِكون من تواجدهم على الإنترنت أو أعادوا توجيهه خوفاً على أمن معلوماتهم الشخصية والمالية وغيرها من المعلومات الخاصة بهم التي تنطوي عليها التفاعلات الرقمية، قد يكون لذلك تأثيرات كبيرة، على كلّ من المنظمات التي لا تتخذ الخطوات الاحترازية اللازمة، وعلى الاقتصاد العالمي الحديث. وعلى العكس، قد تكون التأثيرات ضئيلة لأن المستهلِكين لا يولون إلّا القليل من القيمة لخصوصية معلوماتهم الرقمية أو لا يملكون القوة على التحكُّم في خصوصيتهم.

تُظهر نتائج الدراسة الاستقصائية حول المستهلِكين التي أجريناها أنّ مستوى الوعي بالحوسبة الكمومية ومخاطرها

> أجرينا أيضاً دراسة استقصائية حول المستهلِكين لأن المخاطر التي تعترض التشفير والناجمة عن الحوسبة الكمومية تمتد إلى الاقتصاد العالمي الحديث.

منخفض، وأنّ أكثرية المستهلِكين لم تكن مُكْتَرِثَة لحوادث الأمن الإلكتروني السابقة، ولم تتّخذ غالبية المستهلكين أي خطوة للاستجابة لحوادث الأمن الإلكتروني السابقة. يحتوي الملحق B (ص. 53) على تقريرٍ مفصّلٍ عن نتائج الدراسة الاستقصائية حول المستهلِكين. تتوافق هذه النتائج تقريبيّاً مع الدراسات السابقة حول وجهات نظر المستهلِكين إزاء عمليات اختراق الأمن الإلكتروني. لقد دَرَس أبلون وآخرون (Ablon et al.) (2016) وجهات نظر المستهلِكين ولاحظوا مستويات أعلى من الوعي مقارنةً بتلك التي نعرضها وإنّما مستويات منخفضة مماثلة من الاستجابات المتشدّدة مثل توقُّف التعامل مع الشركات المتأثِّرَة.

علاوةً على ذلك، تشير نتائجنا إلى أنّ المستهلِكين لا يولون إلّا القليل من القيمة لخصوصية معلوماتهم الرقمية أو يملكون قوّة محدودة على التحكّم في خصوصيتهم الرقمية، ولن يغيِّر المستهلِكون سلوكهم إلّا عندما يكون التهديد وشيكاً. تشمل بعض التغييرات في السلوكيات التهديدات التي تتعرّض لها الشركات التي لا تتصرف بشكلٍ استباقيٍّ لحماية خصوصية زبائنها، مثل التغييرات في الولاء للعلامة التجارية. ومع ذلك، تُظهِر النتائج أيضاً أنّ الشركات قد تستطيع التنبؤ بهوية المستهلِكين الذين من المرجّح أن يتوقفوا عن التعامل مع الشركة في حال حدوث تهديدات على الأمن الإلكتروني من خلال فهْم كيفية استجابة الزبائن لعمليات اختراق الأمن الإلكتروني السابقة. بشكلٍ عام، تشير نتائجنا إلى أنّ أي استجابة من المستهلِكين لعمليات اختراق الأمن الإلكتروني السابقة (على سبيل المثال، عملية اختراق تارجت [Target] عام 2013 وعملية اختراق إكويفاكس [Equifax] عام 2017) ترتبط بشكلٍ إيجابيٍّ وملحوظٍ باستجابات نشطة للمستويات المتفاوتة للتهديدات الناجمة عن الحوسبة الكمومية التي نظرنا فيها. بعبارة أخرى، تشير استجابات المستهلِكين لعمليات اختراق الأمن الإلكتروني السابقة إلى مستوى قلَق المستهلِكين بشأن الخصوصية وتُنبئ بالاستجابات المستقبلية. من المرجح أن تتطوّر مواقف المستهلِكين وتوقعاتهم إزاء الأمن الإلكتروني والخصوصية مع تغيُّر البيئة الأمنية في الأعوام الفاصلة بين الحاضر وتاريخ ابتكار حاسوب كمومي، ممّا يتطلّب المزيد من هذه التقييمات بمرور الوقت.

الأفكار المُسْتَنْتَجة الرئيسية لصانعي السياسات: يشير افتقار المستهلكين إلى الوعي بشأن المخاطر الناجمة عن تطوير حاسوب كمّوميّ ذي صلة بالتشفير، وعدم قلقهم إزاء هذا الأمر وعدم استجابتهم له إلى أنّ المستهلِكين إمّا يولون قيمة أقلّ لخصوصيّة معلوماتهم بالمقارنة مع الخدمات التي يتلقّونها بالمقابل، أو يشعرون أنّ القوّة على التحكُّم في خصوصيّة معلوماتهم محدودة. في حين تشير هذه النتائج إلى إمكانيّة تجنُّب التدهورات الشديدة في الثقة بين الشركات والمستهلِكين، إلا أنّها لا تتناسب مع حجم المخاطر التي حدّدها الخبراء ووصفوها. في نهاية المطاف، يشير هذا التباين بين وعي المستهلِكين وحجم المخاطر إلى الحاجة إلى قيادة استباقية من جانِب صانعي السياسات. في حين لا يستحيل فهْم المخاطر، تُشير الطبيعة التقنية للحواسيب الكمومية والتشفير باستخدام المفتاح العام (PKC) ضمناً إلى أنّ بعض المستهلِكين سيختارون عدم دفْع التكاليف المطلوبة لتآلفهم مع القضايا أو لتأييد التغيير في السياسات. وبالتالي، بهدف تجنُّب المخاطر الناجمة عن تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير، يتوجب على صانعي السياسات التصرف بشكلٍ استباقيٍّ لحماية المستهلِكين. قد تكون أعمالٌ مشابهة لعمل يروخيموفيتش وآخرين (Yerukhimovich et al.) (2016) الساعي إلى توجيه صانعي السياسات لوضع لوائح فعّالة تهدف إلى حماية المستهلِكين مفيدة في هذا الصدد.

الأفكار المُسْتَنْتَجة الرئيسية للمنظمات الفردية: تُبيِّن نتائجنا أنّ الاستجابات لعمليات اختراق الأمن الإلكتروني السابقة تشير إلى مستوى قلَق المستهلِكين بشأن الخصوصية وتتنبأ باستجاباتهم المستقبلية، ما يُشير إلى طريقةٍ مُتاحةٍ أمام شركات القطاع الخاص لتُحَسِّن بشكلٍ محتملٍ حساباتها لفوائد الاعتماد الاستباقي والمُبكِر للتشفير ما بعد الكمّ (PQC). في حين يسهل احتساب تكاليف الاعتماد المبكر للتشفير ما بعد الكمّ، تُعتَبَر الفوائد أقل وضوحاً بشكلٍ عام ومقدَّرَة على الأرجح بأدنى من قيمتها. من خلال دمْج استجابات المستهلِكين السابقة لعمليات اختراق الأمن الإلكتروني، قد تتمكَّن شركات القطاع الخاص من التنبؤ بشكلٍ أفضل باستجابات المستهلِكين المرتبطة بالاعتماد الاستباقي والمُبكِر للتشفير ما بعد الكمّ. ويشير هذا إلى فائدتين مُقدَّرَتيْن ربّما

بأدنى من قيمتهما، هما: (1) الفائدة الناتجة عن خسارة عددٍ أقل من الزبائن، و(2) الفائدة الناتجة عن جذْب زبائن المنافسين الأقل استباقيةً والأقل أمناً. في حين لم تُفِد غالبية المستهلِكين باستجابة نشطة لأي من السيناريوهات الافتراضية الثلاثة التي طرحناها، أفادت نسبة 18 في المئة باستجابة نشطة للتهديد "شبه المُحقَّق"، وأفادت نسبة 23 في المئة باستجابة نشطة للتهديد "القائم"، وأفادت نسبة 43 في المئة باستجابة نشطة للتهديد "الوشيك". تُعَرَّف الاستجابات النشطة على أنّها تلك التي تؤثر على قرارات الزبائن بشأن الإنفاق وقد تؤثّر على إيرادات الشركة على الفور.

شواغل ملحوظة أخرى

تمّ استبعاد بعض القضايا من دراستنا، ولكن لا تزال صلتها بالموضوع تستدعي ذِكْرها هنا. تُعتبر تقنيّة توزيع المفاتيح الكموميّة (Quantum Key Distribution [QKD]) أهمّ قضيّة تمّ تحديدها على أنّها خارج نطاق هذا التقرير. تمّت مناقشة تقنيّة توزيع المفاتيح الكموميّة على أنّها حلٌّ مستقبليٌّ فعّالٌ لضمان أمن الاتصالات بطريقة لا تكون فيها عرضة للحواسيب الكمومية. باختصار، تشير تقنيّة توزيع المفاتيح الكموميّة إلى وسيلة لنقل المعلومات التي تعتمد على خواص وسيط الاتصال الميكانيكية الكمومية بحيث يصبح من المستحيل على متنصِّتٍ اعتراض الاتصال من دون علْم المتّصلين. قد ينتج عن ذلك وسيلة لتبادل المفاتيح المتناظرة من دون الخوف من الاعتراض مما قد يمكّن بالتالي إجراء اتصالات مشفّرة تتمتّع بأمن غير ضعيف في وجه الحواسيب الكمومية. في حين تُعتبر هذه التكنولوجيا مثيرة للاهتمام وتُستخدَم بالفعل في عددٍ من تطبيقات العالَم الحقيقي في يومنا هذا، بما في ذلك نظام الأقمار الاصطناعية الصيني ("الأقمار الاصطناعية الصينية تستخدِم التشفير الكمومي لضمان أمن المؤتمرات عبر الفيديو بين القارات،" ["Chinese Satellite Uses Quantum Cryptography for Secure Video Conference Between Continents"]، 2018) وربما في بنية اتصالات الجيل الخامس (5G) التحتية (كوانتم أكستشينج [Quantum Xchange]، 2018)، لا يرى عديدون هذه التكنولوجيا على أنّها بديل مُجدٍ للتشفير ما بعد الكمّ (PQC). وبشكلٍ خاص، يأخذ المركز الوطني للأمن الإلكتروني (National Cyber Security Center)، وهو جزء من مقر الاتصالات الحكومية في المملكة المتحدة (United Kingdom's Government Communications Headquarters) بعين الاعتبار القيود العملية لتوزيع المفاتيح الكموميّة، وخاصة تحديات إمكانية التوسُّع والمرونة، بهدف جعْله بديلاً غير مناسبٍ حالياً للتشفير ما بعد الكمّ لضمان أمن الاتصالات على نطاقٍ واسعٍ في وجه الحواسيب الكمومية (المركز الوطني للأمن الإلكتروني [National Cyber Security Centre]، 2016). بشكلٍ عام، يمكن أن يقال الكثير عن فائدة تقنيّة توزيع المفاتيح الكموميّة والتشفير الكمومي في هذا السياق، غير أنّ مناقشة هذا الموضوع بشكلٍ إضافيٍّ تخرُج عن نطاق هذا التقرير.

التدابير على امتداد الحكومة الأمريكيّة

اتخذت الهيئات على امتداد الحكومة الأمريكية مؤخراً عدداً من التدابير المتعلّقة بالمخاطر الناجمة عن الحوسبة الكمومية، على الرغم من أنّ تركيز هذه التدابير الأوّلي حتى يومنا هذا كان على ضمان ريادة الولايات المتحدة العالمية والحفاظ عليها في مجال التكنولوجيّات الكموميّة. وحتى الآن، لا يُذكَر الخطر على الأمن القومي الناجم عن الحوسبة الكمومية إلّا في عددٍ قليلٍ من النقاط المحدَّدة في التوجيهات والخطط. ولكن، تُعتبر هذه التدابير حديثة نسبياً، وفي معظم الحالات لم تُتَح حتى الآن الفرصة أمام الهيئات الجديدة للخوض بدقّة في تفاصيل أولوياتها أو خطط عملها، لذلك قد تبرز الحاجة إلى إيلاء تداعيات الحوسبة الكمومية على الأمن القومي المزيد من الأولويّة.

لقد تمّ تحفيز معظم التدابير الحكومية من خلال تمرير قانون مبادرة الكمّ الوطنية (National Quantum Initiative Act [NQIA]) في ديسمبر/كانون الأوّل 2018 (مدونة قوانين الولايات المتحدة [U.S.C] 15 الفقرات 8801 – 8852). وقد هَدَفَ قانون مبادرة الكمّ الوطنية صراحةً إلى "ضمان استمرار ريادة الولايات المتحدة في مجال علوم المعلومات الكمومية وتطبيقاتها التكنولوجية." وحقَّقَ القانون هذا الأمر من خلال طلب أنشطة تنسيقية جديدة، وتمويل، ورأس مال بشريّ، وإشرافٍ من جانب الكونغرس على القضايا المتعلقة بعلوم وتكنولوجيا المعلومات الكمومية (Quantum information science and technology [QIST]). وقد أوجد أربع متطلّبات جديدة للسلطة التنفيذية، وهي أن يقوم الرئيس بوضع برنامج مبادرة الكمّ الوطنية (National Quantum Initiative Program [NQIP])، وتأسيس مكتب تنسيق الشؤون الكموميّة الوطني (National Quantum Coordination Office [NQCO])، وتشكيل اللجنة الفرعية لعلوم المعلومات الكمومية (Subcommittee on Quantum Information Science [SCQIS]) تحت لجنة العلوم (Committee on Science) في المجلس الوطني للعلوم والتكنولوجيا (National Science and Technology Council [NSTC])، وتشكيل اللجنة

الاستشارية لمبادرة الكمّ الوطنية (National Quantum Initiative Advisory Committee). كما تضمّنَت الأقسام اللاحقة من قانون مبادرة الكمّ الوطنية المتطلّبات والموارد وبالتحديد بالنسبة إلى المعهد الوطني للمعايير والتكنولوجيا (NIST) ومؤسسة العلوم الوطنية (NSF) ووزارة الطاقة (Department of Energy). بالإضافة إلى المتطلّبات الأخرى، طُلِب من المعهد الوطني للمعايير والتكنولوجيا عقْد "اتحاد كمومي" لأصحاب الشأن من أجل "تحديد المقاييس، والمعايير، والأمن الإلكتروني، والحاجات الأخرى المناسبة في المستقبل" لدعم علوم وتكنولوجيا المعلومات الكمومية.

وتحسّباً لتمرير قانون مبادرة الكمّ الوطنية، اتّخذ البيت الأبيض والمعهد الوطني للمعايير والتكنولوجيا تدابير لتلبية هذه المتطلّبات. فاستجابةً للأوامر التنفيذية والتوجيهات الأخرى، أسّس مكتب سياسات العلوم والتكنولوجيا في البيت الأبيض (The White House Office of Science and Technology Policy [OSTP]) اللجنة الفرعية لعلوم المعلومات الكمومية التابعة للمجلس الوطني للعلوم والتكنولوجيا (NSTC)، واللجنة الاستشارية لمبادرة الكمّ الوطنية، ومكتب تنسيق الشؤون الكموميّة الوطني. يضمّ كلّ من مكتب تنسيق الشؤون الكموميّة الوطني واللجنة الفرعية لعلوم المعلومات الكمومية أعضاء من وكالات فيدراليّة متعدّدة، في حين تضمّ اللجنة الاستشارية لمبادرة الكمّ الوطنية أعضاء من قطاع الصناعة والجامعات والمختبرات الفيدرالية ووكالات فيدراليّة أخرى. إنّ لمكتب تنسيق الشؤون الكموميّة الوطني أهدافاً صريحة متعدّدة، ولكن تجدر الإشارة بشكلٍ خاص إلى أبرز أدواره في الإشراف على التنسيق بين الوكالات، إذ يُعتبر بمثابة نقطة اتصال لتبادُل المعلومات بين الحكومة الفيدرالية، وقطاع الصناعة، والجامعات، والشركاء الآخرين، ويعمل على نشْر التوعية العامة. وبالمثل، للّجنة الفرعيّة لعلوم المعلومات الكموميّة أهدافٌ متعدّدة، ولكنّ تتعلّق تلك التي تهمّ بأدوارها في تنسيق أبحاث علوم وتكنولوجيا المعلومات الكمومية، وتبادُل المعلومات حول تطوير المعايير الدولية واستخدامها، وتقييم احتياجات بنية الحكومة الفيدرالية التحتية، وتقييم الآفاق العالمية من حيث جهود البحث والتطوير في مجال علوم وتكنولوجيا المعلومات الكمومية. ويكمن الأمر المهم في أنّ قانون مبادرة الكمّ الوطنية ينصّ أيضاً على الإشراف على الأنشطة الفيدرالية المتعلقة بعلوم وتكنولوجيا المعلومات الكمومية من خلال مطالبة اللجنة الفرعية لعلوم المعلومات الكمومية بتقديم تقارير منتظمة إلى الكونغرس.

لقد رعى مكتب سياسات العلوم والتكنولوجيا قمة حول علوم وتكنولوجيا المعلومات الكمومية في سبتمبر/أيلول 2018 (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2018b) حيث نشرَت اللجنة الفرعية لعلوم المعلومات الكمومية اللمحة الاستراتيجية الوطنية (National Strategic Overview) الصادرة عنها. تُحدِّد هذه الوثيقة، من بين أمور أخرى، الفُرص في السياسات المتعلِّقة بالحفاظ على الأمن القومي والنمو الاقتصادي. يدعو هذا القسْم الفرعي اللجنة إلى الحفاظ على فهْم التداعيات الأمنية لمشهد العلوم والتكنولوجيا (science and technology [S&T]) المتغيِّر في علوم المعلومات الكمومية (QIS) وتوفير آليات لجميع الوكالات الحكومية لمواكبة التداعيات الدفاعية والأمنية والمساعدة في تحقيق توازُنٍ بين الفوائد والمخاطر الجديدة. يذكُر هذا القسْم الفرعي صراحةً الخطر الذي يعترض التشفير باستخدام المفتاح العام ويشير إلى حاجةٍ إلى الانتقال إلى التشفير ما بعد الكمّ (PQC)، على الرغم من عدم تقديم تفاصيل إضافية. ويذكُر خطوة قادمة رئيسية في تطوير الخطط على مستوى الوكالات والتي قد تشمل "أنظمة الأمن الإلكتروني التحوّلية بما في ذلك التشفير المقاوِم للكمّ استجابةً للتطورات في مجال علوم المعلومات الكمومية." وأخيراً، يشير إلى أنّه طُلب من الوكالات الحكومية وضْع خطط تنفيذيّة مفصَّلة لدعم أنشطة اللجنة، بما في ذلك دعوة أصحاب الشأن للاجتماع "للتشاور مع مكتب سياسات العلوم والتكنولوجيا واللجنة الفرعية لعلوم المعلومات الكمومية من أجل تحديد التحديات الكبرى في مجالات فرعية محدّدة،" بما في ذلك تطوير معايير وأنظمة تشفيريّة مقاوِمة للكمّ (اللجنة الفرعية لعلوم المعلومات الكمومية [Subcommittee on Quantum Information Science]، 2018).

تشير كلّ هذه التدابير إلى أنّ الحكومة الفيدرالية على دراية بالفرص المحتملة لعلوم وتكنولوجيا المعلومات الكمومية وأنّ الهيئات التي تمّ تأسيسها حديثاً لتنسيق عمل الحكومة مركزياً حول هذا الموضوعَ تُدرِك، أقلّه بالحد الأدنى، الحاجة إلى تحويل بنية اتصالاتنا التحتية استجابةً للخطر الناجم عن الحوسبة الكمومية. من المرجّح أن يتطلَّب نطاق التحدي خلال الانتقال إلى التشفير ما بعد الكمّ تنسيقاً مركزيّاً من النوع الذي يهدف برنامج مبادرة الكمّ الوطنية إلى تقديمه، بدلاً من مقاربة تدريجيّة لكلّ وكالة على حدة، على الرغم من أنّه من غير الواضح حتى الآن ما إذا كان برنامج مبادرة الكمّ الوطنيّة يركّز على التهديد بشكلٍ ملائم. ويبدو أنّ تركيز قانون مبادرة الكمّ الوطنية والهيئات التنسيقية الناتجة عنه ينصبّ بشكلٍ حازم على إرساء ريادة الولايات المتّحدة في مجال التكنولوجيا الكمومية، مع إشارات موجزة فقط إلى الاستجابة للتهديد على الأمن القومي، هذا إذا ما تمّ تضمينها أساساً. قد تولي هذه الهيئات التهديد الاهتمام الذي يستدعيه، ولكن ربّما تعود الجهود المبذولة لتحويل بنية معلوماتنا واتصالاتنا التحتية خلال الانتقال إلى التشفير ما بعد الكمّ إلى هيئة مختلفة قد

تُركِّز بشكلٍ أكبر وأحاديٍّ على الشواغل المرتبطة بالأمن الإلكتروني وعلى جهود انتقال تكنولوجيا المعلومات.

لقد أصدر المجلس الاستشاري لاتصالات الأمن القومي (NSTAC) مؤخّراً توصية لمبادرةٍ أوسع، طموحة وابتكارية للأمن الإلكتروني (Cybersecurity Moonshot)، مشيراً إلى أنّ المقاربات التدريجية التي اتخذتها الحكومة الأمريكية في مجال الأمن الإلكتروني بشكلٍ عام غير كافية ويجب وضْع إطار مفاهميّ لمسارٍ جديد. ويوصي بمبادرة طموحة وابتكارية للأمن الإلكتروني، وهي مقاربة على مستوى "الدولة بأكملها" للأمن الإلكتروني تتطلّب أعلى مستوى من الريادة والتنسيق الوطنيين لمواجهة تحديات الأمن الإلكتروني الملّحة الحالية والمستقبلية. يذكُر التقرير تضمين التشفير المقاوِم للكمّ بشكلٍ صريح. ويوصي المجلس الاستشاري لاتصالات الأمن القومي بالتدابير التي يجب على الحكومة الأمريكية أن تتّخذها، بما في ذلك تحديد أهداف طموحة، وتأسيس مجالس مشتركة بين الوكالات ومجالس غير حكوميّة لمواجهة التحديات، وتحديد إطار عمل استراتيجي لأبحاث الأمن الإلكتروني الوطنية وأولويات التطوير (المجلس الاستشاري لاتصالات الأمن القومي، [NSTAC] 2018). في حين دعت منظمات عدّة إلى العمل في مجال الأمن الإلكتروني، يُعتبَر المجلس الاستشاري لاتصالات الأمن القومي فريداً لأنّه لجنة استشارية فيدرالية (Federal Advisory Committee) مرتبطة بالرئيس، تعمل من خلال وزارة الأمن الداخلي (Department of Homeland Security)، وتضمّ أعضاء من قطاع الصناعة. وبالتالي، من المحتمل أن تكون توصيات المجلس الاستشاري لاتصالات الأمن القومي أكثر تأثيراً وفعاليّةً من توصيات المنظمات الأخرى. فقد يشكِّل دمْج الانتقال إلى التشفير ما بعد الكمّ في مقاربة مماثلة للأمن الإلكتروني منسّقة مركزياً، بدلاً من العلوم والتكنولوجيا الكمومية، مقاربة بديلة أفضل لمعالجة المخاطر المحتملة.

تُعتبر استجابة الحكومة الفيدرالية لتحدي العام 2000 والدروس المستفادة من الجهود المبذولة للحد من الخطر المرتبط بها مفيدة أيضاً في تحديد الطرق الفعالة لتحفيز العمل على مستوى الدولة في سياق انتقال تكنولوجيا المعلومات. كان العمل الفيدرالي ضروريّاً لتحفيز العمل الفعال على هذه المشكلة. ففي عام 1997، حدّد مكتب المساءلة الحكومية (Government Accountability Office [GAO]) الانتقال إلى العام 2000 (Y2K) على أنّه مجالٌ عالي المخاطر بالنسبة إلى الحكومة الفيدرالية، وبعد ذلك بوقتٍ قصير بدأت لجان مجلس النواب ومجلس الشيوخ بعقد جلسات استماع حول هذه القضية، وانعقَد مجلس الرئيس بشأن الانتقال إلى العام 2000 (President's Council on Year 2000 Conversion). كان مجلس الرئيس يتألّف من أكثر من 40 مسؤولاً فيدراليّاً أوّلياً، بمَن فيهم نائبي الوزراء، ومديري معلومات (CIOs)، وقيادات عليا أخرى من كلّ إدارة تنفيذية ووكالة حكومية كبرى تقريباً. وفي الأعوام التي تَلَت ذلك وحتى عام 2000، كانت القيادة الفيدرالية مستدامة ومنسَّقة بشأن الاستعداد الوطني للانتقال إلى العام 2000. وعَقَد المجلس أكثر من 100 جلسة استماع للجان الكونغرس حول هذا الموضوع، وأبلغَت الوكالات والإدارات الفيدرالية الرئيسية مكتب الإدارة والموازنة (OMB) بالتقدُّم المُحرَز على أساس فصلي، وتم تأسيس مجموعات عمل قائمة على القطاعات لبناء شراكات مع مجموعات قطاع الصناعة والبنية التحتية الأساسية. كما تمّ تمرير تشريع من قِبَل الحزبين، تَمَثَّل بقانون الإفصاح عن معلومات الانتقال إلى العام 2000 والجهوزية له (Year 2000 Information and Readiness Disclosure Act)، بهدف التأسيس للرقابة والتنظيم والتحفيز للاستعداد. كما تركّزَت الجهود المبذولة على التأييد ورفْع مستوى الوعي أولاً، ثم على المساعدة في التوجيه بشأن تقييم المخاطر، وأخيراً على الاستعداد والتخطيط للطوارئ. في نهاية المطاف، أدّت هذه الجهود إلى جهود منسَّقة ومستدامة مبذولة على مستوى الدولة للتخفيف من المخاطر على امتداد الحكومة الفيدرالية والصناعات الرئيسية، ولم تتحقّق الأعطال التي كان يُخشى أن تحدث بسبب الانتقال إلى العام 2000 البتة. في وقتٍ لاحق، أفاد مكتب المساءلة الحكومية بالدروس الرئيسية المستفادة من جهود الحكومة الفيدرالية. كان من أهمها أنّ القيادة الفيدرالية والشراكات كانت أساسية للنجاح، وخاصةً القيادة المركزية والتنسيق والرقابة من قِبَل حزبي الكونغرس على السلطة التنفيذيّة. وقد أدّى ذلك بدوره إلى شراكات ناجحة مع الولايات والمدن والمجموعات الصناعية، وإلى تشريعات مفيدة، وتخصيص رأس المال البشري والموارد اللازمة لمساعدة الكيانات على الاستعداد. وفي حين أنّ هناك أوجه فرْق ملحوظة بين التهديد الناجم عن الانتقال إلى العام 2000 والتهديد الناجم عن الحواسيب الكمومية، لا سيما فيما يتعلّق بالتاريخ المحدَّد للضعف ووجود خصْم قادر تقنياً، توفِّر هذه الجهود رغم ذلك نموذجاً مفيداً يمكن تكييفه في سياق الجهد القادم المبذول على نطاق الدولة والرامي إلى التخفيف من المخاطر والذي يجب أن يُرافِق الانتقال إلى التشفير ما بعد الكمّ (مكتب المساءلة الحكومية [GAO]، 2000). لقد أثبَتَ الكونغرس أصلاً استعداده لمعالجة المخاطر الناجمة عن الحوسبة الكمومية بأسلوب مماثل يشمل الحزبين، ويبدو أنّ عدداً من الهيئات التي تمّ تأسيسها نتيجةً لبرنامج مبادرة الكمّ الوطنية يتمتّع بوضعيّة جيّدةٍ لإحداث تنسيقٍ فعّالٍ للغاية بين الوكالات وبين الحكومة الفيدرالية والمجتمع المدني حول التشفير ما بعد الكمّ يكون شبيهاً بالتنسيق الذي تمّ استجابةً للانتقال إلى العام 2000. ومع ذلك، يبقى أن نرى

ما إذا ستركّز أولويات السلطة التنفيذية ورقابة الكونغرس جهود برنامج مبادرة الكمّ الوطنية حول تغييرات تكنولوجيا المعلومات بشكلٍ ملائمٍ مستخدمةً هذه الهيئات الأكثر تركيزاً بشكلٍ صريحٍ على ريادة الولايات المتحدة في مجال العلوم وتكنولوجيا الكمّ.

التوصيات

النتائج المُستخلصة الرئيسيّة

يبدأ هذا القسم بتلخيص نتائج هذه الدراسة المُستخلصة الرئيسية، بالاستناد إلى توليف المقابلات التي أجريناها مع الخبراء، ومراجعة الدراسات السابقة، والدراسة الاستقصائيّة حول المستهلكين. بشكلٍ عام، نَجِد أنّ استجابة الولايات المتحدة تتطلّب ثلاث مقاربات واسعة ومتداخلة، وهي:

تحفيز اعتمادٍ قويٍّ للتشفير ما بعد الكمّ (PQC) في أقرب وقتٍ ممكن. سيشكّل اعتماد التشفير ما بعد الكمّ بشكلٍ آنيٍّ (في حينه) وقويٍّ وكاملٍ المسار الأفضل الوحيد للتخفيف من الخطر الناجم عن الحواسيب الكمومية. من المرجَّح أن يكون التشفير ما بعد الكمّ وسيلةً فعّالةً لضمان أمن الأنظمة في وجْه تهديد ناجم عن الحواسيب الكمومية، غير أنّ عمليات الانتقال إلى التشفير الكاملة تستغرق أعواماً عديدة، ويتعرّض بعض المنظمات الذي يملك معلومات حسّاسة طويلة الأجل أصلاً للخطر. كلّما اقتَرَبَت إمكانية تطبيق معيار قابلٍ للتشغيل المتبادل للتشفير ما بعد الكمّ على نطاقٍ واسع، قلَّ الخطر في نهاية المطاف.

إدماج المرونة الإلكترونية وسرعة التشفير في البنية التحتية الرقمية. مع تكييف تطبيقات الأمن استجابةً للتهديدات الحالية المتطوِّرة باستمرار على بنيتنا التحتية وللتهديدات المستقبلية مثل الحوسبة الكمّومية على حدّ سواء، يجب أن ننظُر في كيفية جعْل تطبيقات الأمن الجديدة أكثر سرعة. وبشكلٍ محدَّد، يجب أن تهدف الأنظمة الجديدة إلى (1) تحقيق التوافق المستقبلي مع التطوُّر المُتَوَقَّع لمعايير التشفير ما بعد الكمّ (PQC) ومقتضياته الأكثر تطلُّباً، و(2) تطبيق النمطية التي قد تسمح بتكييف سريع وغير مكلف للتشفير مع اكتشاف تهديدات أو نقاط ضعْف جديدة. توفِّر التغييرات المنهجيّة اللازمة للانتقال إلى التشفير ما بعد الكمّ فرصة لتطبيق تحسينات هيكلية في كيفية استخدام التشفير في أنظمة الاتصالات والمعلومات التي قد تحسِّن قدرتنا على الاستجابة للتهديدات الإلكترونية الحالية والمستقبلية على حدّ سواء. يجب أن يكون الهدف الترادفي من الجهود الرامية إلى تعزيز اعتماد التشفير ما بعد الكمّ والاستعداد للحوسبة الكمومية إعادة هيكلة الأنظمة من أجل تمكين المزيد من المرونة الإلكترونية وسرعة التشفير.

تطوير خطط لجهوزيّة أمن المعلومات لمستقبلٍ مجهول. تطرح الإمكانيات في تقدُّم الجداول الزمنيّة لتطوير حاسوبٍ كمّوميٍّ ذي صلة بالتشفير واعتماد التشفير ما بعد الكمّ حالة من عدم اليقين بالنسبة إلى المكلَّفين بمهمّة الاستعداد للتهديدات الأمنية المستقبلية. يسود عدم اليقين حول موعد ظهور الحواسيب الكمومية، ومدى سرعة اعتماد التشفير ما بعد الكمّ، وحول ما يتطلّبه الأمر بالنسبة إلى المنظمات الفردية والولايات المتحدة ككلّ للاستعداد، ومدى شدّة الخطر على مستوى المجموعة والفرد. من الممكن حدوث مفاجآت في الجداول الزمنية المرتبطة بالاعتماد الباكر أو المُتأخِّر، ولكنّها غير مرجحة. ولكن، يجب ألا يكون مستقبلٌ غير مؤكّد مستقبلاً أقل أمناً.

يجب أن تسعى الرسائل الموجَّهة إلى الجمهور بشأن الخطر الناجم عن الحواسيب الكمومية إلى إيجاد حلٍ وسطيٍّ بين المبالغة في التهديد والتجاهل المتهور للخطر الحقيقي. تمتلك الولايات المتحدة حلولاً للتخفيف من المخاطر، ولن يؤدّي حتى أسوأ السيناريوهات إلى نهاية أمن المعلومات الرقمية. وفي أفضل السيناريوهات، قد يتحسَّن الأمن الإلكتروني عالمياً. من الضروري تشجيع تقييمات معقولة لمخاطر التهديد التي تؤدّي إلى اتخاذ التدابير الملائمة. تهدف هذه المقاربة إلى تجنُّب التصريحات التخويفيّة غير الضروريّة. فعلى سبيل المثال، لا تُعتبر الحوسبة الكمومية "نهاية الخصوصية" (كامبل [Campbell]، 2018)، وفي جميع الترجيحات، لن "تَخرُق على الفور تشفير البيانات الحسّاسة المحمية بأقوى أنظمة الأمن الحالية ... في فترة تزيد بقليل عن خمسة أعوام" (فورمسكي [Foremski]، 2018). ومع ذلك، يُعتبَر خطراً حقيقيّاً يمكن ويجب الاستعداد له. ينبغي الحد من حالات عدم اليقين متى وحيثما أمكن ويجب تحديث أنشطة إدارة المخاطر وفقاً لذلك.

أبرز التوصيات

السلطة التنفيذية

إذا كان البيت الأبيض يرغب في الحدّ من الخطر الناجم عن الحوسبة الكمومية، فعليه أن يأخذ التوصيات الأربع التالية في عين الاعتبار:

1. النظر فيما إذا كان باستطاعة الهيئات التي تمّ تأسيسها لتكون جزءاً من مبادرة الكم الوطنية (National Quantum Initiative) أن تولي أولوية كافية لاستجابةٍ على مستوى الدولة بأكملها للتهديد الناجم عن الحوسبة الكمومية.

سيتطلب التخفيف من المخاطر التي تتعرض لها بنية اتصالاتنا التحتية نتيجة الحوسبة الكمومية قيادة وتنسيقاً

وإشرافاً مستداماً من السلطة التنفيذية، على أن تبدأ هذه الأمور فوراً وتستمرّ حتى وقت طويل بعد تطوير حواسيب كمومية ذات صلة بالتشفير. يبدو أنّ مكتب تنسيق الشؤون الكمومية الوطني (NQCO) التابع لمكتب سياسات العلوم والتكنولوجيا (OSTP)، واللجنة الاستشارية لمبادرة الكمّ الوطنية (National Quantum Initiative Advisory Committee)، واللجنة الفرعية لعلوم المعلومات الكمومية في المجلس الوطني للعلوم والتكنولوجيا (NSTC SCQIS) في وضعية جيّدة أساساً لتوفير الريادة، وتعزيز التنسيق بين الوكالات، وتقييم الخطر، وبناء الشراكات اللازمة بين الحكومة الفيدرالية والجهات الفاعلة الأخرى، باتّباع الدروس المستفادة من نجاحات مجلس الرئيس بشأن الانتقال إلى العام 2000 (President's Council on Y2K Conversion). ومع ذلك، ما زال من غير الواضح ما إذا كانت هذه المنظمات مركَّزة بشكلٍ كافٍ على الاستجابة للخطر الناجم عن الحوسبة الكمومية والذي يهدّد بنية المعلومات والاتصالات التحتية الخاصّة بنا. يتوجب على البيت الأبيض النظر فيما إذا كانت هذه الهيئات، التي تمّ تشكيلها لهدف صريح ألا وهو ضمان ريادة الولايات المتّحدة في علوم وتكنولوجيا (S&T) المعلومات الكمومية، هي أنسب الكيانات لإدارة هذا الخطر، بدلاً من هيئات تتمتّع بوضعيّة مماثلة والتي تركّز بشكلٍ أحاديّ على الأمن الإلكتروني وتحويل تكنولوجيا المعلومات و/أو الأمن القومي.

2. ضمان إصدار معيار التشفير ما بعد الكمّ (PQC) النهائي في الموعد المحدَّد واستمرار منْح الأولوية لتسهيل الاعتماد على نطاقٍ واسع.

ستؤثر الحالة النهائية لمعيار التشفير ما بعد الكمّ (PQC) الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST) على معدّل اعتماد المعيار في نهاية المطاف. يبدو أنّ نشاط المعهد الوطني للمعايير والتكنولوجيا لتوحيد معايير التشفير ما بعد الكمّ يفضّل أصلاً وبدرجة كبيرة، في معايير التقييم الخاصة به، ميزات المعيار النهائي التي ستُسهّل الاعتماد على نطاقٍ واسع. ومن بين أمور أخرى، ذَكَر المعهد صراحةً أنّه يُفضّل عوامِل مثل أحجام أصغر للمفاتيح وفعاليّة الخوارزميات الحسابية التي ستحدّ من التكلفة الإجمالية. تشير المعايير أيضاً إلى تفضيلٍ قويٍّ للخوارزميات التي يمكن ترخيصها من دون تعويض. سيشكّل كلّ ذلك عوامِل مهمة في تسهيل اعتماد المعيار في نهاية المطاف.

تشير الإعلانات المتعلّقة بنشاط توحيد المعايير إلى أنّه من المنوي أن يكون المعيار متاحاً في جميع أنحاء العالم، ونوصي بأن يتابع المعهد الوطني للمعايير والتكنولوجيا هذه النيّة من خلال رفعه إلى المنظّمة الدولية لتوحيد المقاييس (ISO) لجعله معياراً دولياً. علاوةً على ذلك، في حين تشير الوثائق إلى أنّ المعهد الوطني للمعايير والتكنولوجيا قد يحتاج إلى توحيد أكثر من نوعٍ واحدٍ من كل خوارزمية، يجب أن يحرص النشاط على تقليص العدد الإجمالي لكلّ نوع مُختار من الخوارزميات لتجنُّب تجزئة السوق. أخيراً، نظراً لأنّ إصدار معيار التشفير ما بعد الكمّ يُرجّح أن يكون بمثابة "طلقة البداية" للانتقال العالمي إلى التشفير ما بعد الكمّ، فمن الضروري توفير التمويل الكافي وإيلاء الأولويّة المناسبة للجهود من أجل إنهاء نشاط توحيد المعايير في الموعد المحدَّد.

3. يجب أن تنظر وكالة الأمن القومي (NSA) في فرْض انتقال الحكومة الفيدرالية، والبنية التحتية الأساسيّة، والمنظمات التي تقدّم منتجات إلى الحكومة إلى التشفير ما بعد الكمّ (PQC) وإنفاذه بقوّة.

إنّنا نتوقّع أنْ تُواصل مديرية الأمن الإلكتروني في وكالة الأمن القومي (NSA Cybersecurity Directorate) والمعهد الوطني للمعايير والتكنولوجيا (NIST) العمل معاً عند إصدار معيار التشفير ما بعد الكمّ النهائي للدفع بعملية الانتقال إلى التشفير ما بعد الكمّ (PQC) على امتداد الحكومة الفيدرالية. وقد أشارَت أصلاً مديريّة ضمان أمن المعلومات (IAD) في وكالة الأمن القومي إلى أنّها ستستعِدّ للقيام بذلك عندما أوصت بوقف الجهد المستمرّ الرامي إلى الانتقال إلى التشفير بالمنحنيات الإهليلجية في عام 2016. وفي سياق هذا الجهد، يجب على وكالة الأمن القومي النظر في فرْض انتقال الحكومة والبنية التحتية الأساسية إلى التشفير ما بعد الكمّ. قد يتطلّب فرْض الانتقال أيضاً أن يكون التشفير ما بعد الكمّ افتراضياً لدى جميع الشركات التي تبيع المعدّات الحاسوبيّة أو البرمجيّات للزبائن الحكوميين، ما يستدعي في نهاية المطاف استبدال أي منتجات تستخدم خوارزميات التشفير باستخدام المفتاح العام الحالية. ولكن، لكي تكون إجراءات الفرْض هذه فعّالة، يجب أن يكون الإنفاذ متسقاً وقويّاً. يشير رأي الخبراء إلى أنّ الانتقال الأخير بقيادة الحكومة إلى التشفير بالمنحنيات الاهليلجية لم يتمّ إنفاذه بشكلٍ كافٍ على جميع الأطراف، بما في ذلك شركات البرمجيات، وهيئات إصدار الشهادات، ومقدمي الخدمات السحابية، وكثيراً ما تمّ منْح إعفاءات من توفيره. لذلك، يجب إنفاذ إجراءات فرْض التشفير ما بعد الكمّ بشكل مناسب على جميع أصحاب الشأن، مع منْح أقل عدد ممكن من الإعفاءات.

4. بدء التنسيق بين الوكالات وبناء الشراكات بين القطاعين العام والخاص مع التركيز على الدفع باتجاه التغيير ورصدْه للتخفيف من الخطر الناجم عن الحوسبة الكمومية على نطاق الدولة، وتوسيع نطاق التنسيق والشراكات.

سواء اعتُبرت الهيئات التي تم تشكيلها لتكون جزءاً من

برنامج مبادرة الكمّ الوطنيّة (NQIP) كافية أم لم تكن لتركيز الجهد الوطني على التخفيف من المخاطر الناجمة عن الحواسيب الكمومية ووضعه على سلّم الأولويّات، من الملحّ أن تبدأ قريباً هيئة مختارة باتخاذ التدابير لبدء العمل المشترك بين الوكالات وتوسيعه وبناء شراكات بين القطاعين العامّ والخاص. من أجل التبسيط، نفترض هنا أنّ مكتب تنسيق الشؤون الكمومية الوطني (NQCO) سيكون الهيئة التنسيقية المُختارَة، على الرغم من أنّ هيئةً أخرى قد تكون أكثر ملاءَمةً للاضطلاع بهذا الدور، تماشياً مع التوصية الأولى هنا. في حين يُحدِّد قانون مبادرة الكمّ الوطنية (NQIA) عدداً من الوكالات والإدارات لتكون ممثَّلة في مكتب تنسيق الشؤون الكمومية الوطني وفي اللجنة الفرعية لعلوم المعلومات الكمومية (SCQIS)، تبقى هذه القائمة محدودة للغاية، ويجب توسيع التنسيق ليشمل ممثلين من عددٍ أكبر من الوكالات والمنظمات على امتداد الحكومة الفيدرالية. يُلاحَظ غياب وكالة الأمن الإلكتروني وأمن البنية التحتية (CISA) عن قائمة المنظمات الأعضاء المطلوبة، نظراً لدورها في الدعوة إلى الاجتماع ومسؤوليّتها في التنسيق بين الحكومة ومنظمات القطاع الخاص على نطاقٍ واسعٍ لتوفير حماية إلكترونية شاملة وبناء مرونة البنية التحتيةً وإدارة المخاطر الوطنية. ويمكن، لا بل ينبغي، أن يتمّ تمثيل موظفي المنظمات الأخرى، بما في ذلك على سبيل المثال لا الحصر، موظفي كلّ إدارة رئيسية تابعة للسلطة التنفيذية وموظّفي المنظمات ذات الاختصاصات في قطاعات محدَّدة أو في مجال البنية التحتية الأساسية، مثل الإدارة القومية للاتصالات والمعلومات (NTIA) ولجنة الأوراق الماليّة والصرف الأمريكيّة (SEC) ولجنة التجارة الفيدرالية (FTC). لقد اعتُبِرت مجموعة مثل مجلس مديري المعلومات (CIO Council)، المُكوَّن من مديري المعلومات ونائبيهم في إدارات ووكالات فيدرالية مُتعدِّدة، هيئةً قيّمة بشكلٍ خاصّ في تنسيق الاستجابة للانتقال إلى العام 2000 (Y2K)، وينبغي النظر جدّياً أيضاً في انخراط هذه المجموعة.

يجب على كلّ إدارة أو وكالة عضو أن تُخطِّط لرفع تقرير مُنتظم حول التقدُّم المحرَز في إعداد بنيتها التحتية للحواسيب الكمومية وأن تشارِك كيفية معالجتها للقضايا المهمة مثل عمليات الانتقال إلى سرعة أكبر في التشفير. يتوجّب على مكتب تنسيق الشؤون الكمومية الوطني تأسيس مجموعات عمل تُقدِّم بانتظام تحديثات حول التدابير المُتَّخذة من الإدارات والوكالات الأعضاء لبناء شراكات وتأييد هذه القضية مع المنظمات والمجموعات التجارية وأصحاب الشأن الآخرين ضمن نطاق اختصاصهم. ويجب منْح مجموعات العمل القائمة على القطاعات والمنظمات الفردية استقلاليةً كافيةً لتحديد الطريقة الأكثر ملاءمةً لأداء مهامها الأوسع نطاقاً مع أصحاب الشأن المعنيين، بحيث ستختلف الاستراتيجيات من منظّمة إلى أخرى. قد تحتاج الوكالات إلى تأسيس فِرق عمل خاصة بها، ورعاية التمويل، وبناء شراكات صناعية. على سبيل المثال، في عام 1998، بدأت لجنة التجارة الفيدرالية بذْل جهدٍ خاصٍ لتوعية شركات الأعمال والمستهلِكين سعت من خلاله إلى الحصول على تعليقات من الجمهور العام حول تأثير الانتقال إلى العام 2000 (Y2K) على الخدمات المالية والمنتجات الاستهلاكية. اجْتَمَعَت اللجنة بانتظامٍ مع المجموعات الصناعية ومجموعات المستهلِكين ووضَعَت تنبيهات موجَّهة إلى شركات الأعمال مع إرشادات حول جهوزيّة قطاع الصناعة. وبالمثل، دخلَت لجنة الأوراق الماليّة والصرف الأمريكيّة في شراكة مع رابطة صناعة الأوراق المالية (Securities Industry Association)، ومعهد شركات الاستثمار (Investment Company Institute)، والرابطة الوطنية للمتاجرين بالأوراق المالية (National Association of Securities Dealers)، وأصدرَت نشرات تفسيرية تُحدِّد كيفية تلبية الشركات التزامات الإفصاح (لجنة الأوراق الماليّة والصرف الأمريكيّة [SEC]، 1999). يجب القيام بأنشطة توعية واتخاذ تدابير مماثلة استجابةً للانتقال إلى التشفير ما بعد الكمّ (PQC)، على امتداد كلّ الإدارات والوكالات، حيث أشار تقرير مكتب المساءلة الحكومية (GAO) حول الانتقال إلى العام 2000 إلى أنّ الشراكات التي تمّ تشكيلها وسُبل الاتصال المتعدّدة فيما بينها شَكَّلَت عواملَ مُهمة في النجاح الشامل.

ومع اقتراب إصدار بروتوكولات التشفير ما بعد الكمّ المعياريّة، يجب أن تصبح التقارير أكثر تواتراً، وأن تتَّسِع المهمة لتشمل أيضاً رصْد التقدُّم المحرَز في الانتقال إلى التشفير ما بعد الكمّ وتقييمه. وأخيراً، مع تحسُّن قدرة الحوسبة الكمومية، يجب أن ينظر مكتب تنسيق الشؤون الكمومية الوطني في التحرّك نحو التركيز على التخطيط للطوارئ والاستجابة لها. ستكون هذه الجهود قيِّمة في توفير نقطة محوريّة للتنسيق بين الوكالات، وتعاوُن القطاع الخاص، والتركيز المستدام على القضية ما دامت الحاجة تدعو إلى ذلك، وينبغي أن تُركِّز الرسائل طوال الجهد المبذول على فرصة استخدام إعادة التشكيل المحفوفة بالتحديات والضروريّة للانتقال إلى التشفير ما بعد الكمّ بهدف التحوّل عمداً نحو وضْعٍ مستقبليّ أكثر استدامةً وأمناً.

السلطة التشريعية

من المرجح أن تكون تدابير حزبي الكونغرس المستدامة بالغة الأهمية لنجاح استجابة الحكومة للخطر الناجم عن الحوسبة الكمومية. لقد اتَّخَذ الكونغرس خطوةً أولى ممتازة مع تمرير قانون مبادرة الكمّ الوطنية (NQIA)، ولكن من المرجّح أن

تدعو الحاجة إلى اتخاذ تدابير وإجراء رقابة إضافية لمعالجة الخطر مع اقتراب تطوير الحواسيب الكمومية ذات الصلة بالتشفير. إذا رَغِبَ الكونغرس في تعزيز الوعي حول الخطر الناجم عن الحوسبة الكمومية وزيادة الرقابة على جهود الاستعداد، عليه أن ينظر في التوصيتين التاليتين:

5. عقْدُ جلسات استماع لتحسين الوعي والرقابة.

قد تعزّز جلسات الاستماع في الكونغرس الوعي حول الخطر الناجم عن الحوسبة الكمومية، وإرساء الرقابة، ورصْد التقدُّم المُحرَز نحو الاستعداد للحواسيب الكمومية. ويجب على لجان الكونغرس، ولا سيما لجنة الرقابة والإصلاح الحكومي في مجلس النواب الأمريكي (House Committee on Oversight and Government Reform) ولجانها الفرعية المعنية بتكنولوجيا المعلومات والأمن القومي ولجنة الأمن الداخلي والشؤون الحكومية في مجلس الشيوخ الأمريكي (Senate Committee on Homeland Security and Governmental Affairs) ولجنتها الفرعية المعنية بالشؤون التنظيمية والإدارة الفيدرالية النظر في عقْد جلسات استماع على الفور حول هذا الموضوع. ويجب أن ينصَب التركيز الفوري على المنظمات التي تواجه القدر الأكبر من الخطر الناجم عن نقاط ضعْف الالتقاط والاستغلال وعلى جهوزية الوكالة للانتقال إلى التشفير ما بعد الكمّ وعلى سرعة أكبر في التشفير. بشكلٍ خاص، يجب على اللجان أن تولي اهتماماً خاصاً لعدم وضوح الخط الفاصل بين منظمات الأمن القومي وغير القومي، بحيث لا يزال باستطاعة المهاجمين الساعين وراء أهداف أقلّ حصانةً تُعنى بوظائف أساسيّة مثل معالجة عمليات الدفع وإدارة السجلات أن يتسبّبوا بأعطالٍ وأضرارٍ كبيرةٍ بالأمن القومي إذا كانت غير محميّة. اعتُبِرت مخرجات اللجنة الفرعية المعنية بإدارة الشؤون الحكومية والمعلومات والتكنولوجيا التابعة للجنة الإصلاح الحكومي في مجلس النواب الأمريكي (House Subcommittee on Government Management, Information and Technology of the Committee on Government Reform)، وخاصة المقاييس البارزة لاستجابات الوكالات، عوامِل محفّزة ممتازة في الاستجابة للانتقال إلى العام 2000 (Y2K) (مكتب المساءلة الحكومية [GAO]، 2000). يجب أن تستمر لجان الكونغرس في عقْد جلسات استماع منتظمة بمرور الوقت وطلب تقارير من الوكالات بهدف رصْد التقدُّم المحرَز في سياق الجهود المبذولة وتوفير الرقابة.

6. تنظيم الانتقال إلى التشفير في القطاعين العام والخاص وتحفيزه ودعمْه.

بمجرد توفُّر بروتوكولات التشفير ما بعد الكمّ (PQC) المعياريّة، يتوجّب على الكونغرس النظر في اتّخاذ عددٍ من التدابير الإضافية لوضع لوائح فعّالة وإنفاذها وفرْض الاعتماد على نطاقٍ واسع وتحفيزه. قد يؤدّي الاتكال على قوى السوق لدفع المنظمات التجارية إلى الاعتماد إلى امتناع الشركات عن الاعتماد إلى حين يتمّ اختراقها، في حين يمكن لانتقال بقيادة الحكومة أن يفرض إجراءات أكثر استباقية. بافتراض أنّ وكالة الأمن القومي (NSA) تفرض انتقال الحكومة، والبنية التحتية الأساسيّة، ومزوّدي الحكومة التجاريين إلى التشفير ما بعد الكمّ (راجع التوصية رقم 3)، يجب أن يرصد الكونغرس التقدُّم وأن يكون جاهزاً لوضْع المزيد من اللوائح وإجراءات الفرض بالنسبة إلى الحكومة أو البنية التحتية الأساسيّة، بحسب الحاجة لتعزيز اعتمادٍ سريعٍ وقويٍّ للتشفير ما بعد الكمّ. بالنسبة إلى البنية التحتية الأساسيّة المُنظَّمة أصلاً بشكلٍ صارم، قد تكون المسألة متعلّقة بجعل التشفير ما بعد الكمّ أولوية بالنسبة إلى أولائك الأفراد أو تلك المنظمات التي تضمن أصلاً الامتثال للّوائح. بالإضافة إلى ذلك، ثمّة فرق بين فرْض الانتقال وضمان تطبيق الأنظمة الجديدة الملائم، وينبغي أن ينظر الكونغرس في نهاية المطاف في التشريع الذي قد يوفّر مخططاً لإصدار الشهادات لتطبيقات التشفير ما بعد الكمّ.

اعتماداً على نطاق التغييرات المطلوبة في النهاية، قد يكون الانتقال إلى التشفير ما بعد الكمّ أكثر صعوبةً وتكلفةً بالنسبة إلى بعض المنظمات الحكومية مقارنةً بغيرها. لقد خصَّص الكونغرس التمويل ورأس المال البشري لدعم برنامج مبادرة الكمّ الوطنية (National Quantum Initiative Program)، غير أنّ تركيز قانون مبادرة الكمّ الوطنية (NQIA) انصبّ على ريادة الولايات المتّحدة في مجال علوم وتكنولوجيا المعلومات الكمومية على نطاقٍ واسع. يتوجب على الكونغرس النظر فيما إذا كان من الضروري تخصيص الأموال ورأس المال البشري للاستعداد للحاسوب الكمومي بشكل محدَّد (أي تعزيز التحرّك نحو سرعة التشفير والانتقال إلى التشفير ما بعد الكمّ) على امتداد الحكومة. أخيراً، بالنسبة إلى القطاعات التجارية أو شركات الأعمال التي لا تتأثر بفرْض وكالة الأمن القومي، يجب على الكونغرس النظر في الحوافز التجارية التي قد يتمّ تقديمها لتعزيز اعتماد التشفير ما بعد الكمّ على امتداد الدولة بشكلٍ إضافيّ.

المنظمات الفردية

إذا رَغِبَت المنظمات في الحدّ من المخاطر، عليها أن تنظر في التوصيات الثلاث التالية:

7. تقييم الخطر المستقبلي والرجعي الناجم عن الحواسيب الكموميّة.

يجب أن تكون المنظّمات الفرديّة حالياً في طور تقييم المخاطر الخاصة بها والناجمة عن الحوسبة الكمومية ووضْع الخطط لإدماج التشفير ما بعد الكمّ (PQC) في إدارة أمن دورة حياتها، حيثما كان ذلك مناسباً. ستختلف نتائج

هذا الأمر إلى حدٍّ كبيرٍ من منظمة إلى أخرى. يجب على المنظمات تقييم نقاط الضعف الحالية والمستقبلية، بما في ذلك تلك الناتجة عن المعلومات التي تمّ التقاطها أصلاً أو يجوز التقاطها الآن واستغلالها بعد أعوام. قد يواجه عدد من المنظمات أصلاً خطراً نتيجة الضعف الآنف ذكره، وسينمو هذا الخطر كلّما استغرق الانتقال إلى التشفير ما بعد الكمّ فترة أطول. يجب أن يصبح الخطر الناجم عن الحواسيب الكمومية جزءاً من تقييم المخاطر التنظيمية، وأن تأخذ التقييمات في الاعتبار تفاصيلٍ مثل تحديد المعلومات التي تمّ نقلها والمحميّة حالياً بالتشفير باستخدام المفتاح العام، والمدة التي يجب خلالها أن تبقى تلك المعلومات سريّة، وهويّة الجهات المُهَدِّدة التي قد تستخدِم تلك المعلومات لإلحاق الضرر بالمنظمة. أخيراً، يجب أن تتضمن التقييمات تحديثات منتظمة استناداً إلى مراحل التطوير الرئيسية الجديدة التي تفضي إلى ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير.

8. جردُ استعمالات التشفير باستخدام المفتاح العام. يجب أن تنظر المنظمات في البدء بجرْد كلّ مكان يُستخدم فيه التشفير باستخدام المفتاح العام. فيجب عليها تقييم الأماكن حيث تتفاعل مع التشفير باستخدام المفتاح العام وخاصةً حيث تكون المسؤولية أو السيطرة في أيدي أطراف ثالثة، أو شركاء، أو مورّدين. ستحتاج كلّ عقدة في نهاية المطاف إلى الانتقال إلى التشفير ما بعد الكمّ (PQC) بمجرد توفُّر المعايير. قد يكون الانتقال بسيطاً بحيث يتطلّب من بعض المنظّمات مجرّد تحديث البرمجيّات، أو معقداً بحيث يحتاج مثلاً إلى استبدال المئات أو الآلاف من قِطَع المعدّات الحاسوبية أو تحديث تطبيقات متعدّدة. وكلّما ازدادت الحاجة تعقيداً، وَجَبَ على المنظمة أن تسارِع في بدء معالجتها لضمان جهوزيتها.

9. بناء المرونة الإلكترونية وسرعة التشفير. سيتطلّب التهديد الناجم عن الحوسبة الكمومية تغييراً معقداً وصعباً ومنهجياً في بنية التشفير التحتية، ولكنّه يوفّر أيضاً فرصة. من المفترض أن يتيح للولايات المتحدة، لا بل يستوجب منها، إجراء تغييرات جَماعية ستسهّل تطوير عمليات التشفير المستقبلية وستحسِّن الأداء وستتيح بناء سرعة ومرونة إلكترونية أكبر. يجب على المجموعات الصناعية النظر في الدراسات والمنشورات التي تحدِّد لدوائرها الجَماهيريّة وتفسّر لها الفوائد على مستوى قطاع الصناعة في مجال الأمن والأداء والتي يمكن توقّعها نتيجةً لسرعةٍ أكبر في التشفير. يجب أن تشير الرسائل حول الانتقال إلى التشفير ما بعد الكمّ (PQC) وحتمية عمليات الانتقال المستقبلية إلى الفرصة التي يوفِّرها هذا الانتقال لإدماج التغييرات في الاستخدام العام للتشفير، ما قد يكون مفيداً لقطاع الصناعة ككلّ. ويتوجّب على المجموعات الصناعية النظر في بناء شراكات مع الإدارات والوكالات الفيدرالية المكلَّفة بتعزيز المرونة الإلكترونية وإدارة المخاطر، خاصةً فيما يتعلّق بالحوسبة الكمومية.

وفي حالات متعدّدة، سيتوجّب على المطوّرين والمخططين المسؤولين عن تطبيق الأمن في المنظمات أن يكونوا أكثر دراية بسرعة التشفير. ينبغي ألا يشمل هذا الفوائد المحتملة والمقاربات لسرعة التشفير فحسب، بل أن يتضمن أيضاً توصيات لتجنُّب الصعوبات المحتملة، مع إيلاء اهتمامٍ خاص للقضايا المحتملة المتعلقة بازدياد التعقيد والتحجّر. وفي شركات الأعمال الأكبر، قد يشمل ذلك بشكلٍ رئيسيٍ مدير المعلومات (CIO)، أو مدير الأمن (Chief Security Officer)، أو مدير أمن المعلومات (Chief Information Security Officer)، أو المشفّرين، أو مطوري التطبيقات التي تستخدِم التشفير. سوف تستفيد شركات الأعمال الأصغر أيضاً من الأفراد الذين يؤدون أدواراً مماثلة من خلال استخدام تقارير المعهد الوطني للمعايير والتكنولوجيا (NIST) ووثائق توجيهية أخرى لتصبح أكثر دراية بالموضوع.

ويجب على أولئك الذين يطورون تطبيقات جديدة أن يخطِّطوا على وجه التحديد للمنتجات مع أخْذ السرعة وسهولة الانتقال والتوافق المستقبلي في الاعتبار. ويجب أن تخطِّط الجهات المُنَفِّذَة لعمليات الانتقال القادمة لدى تطبيقها التغييرات للانتقال إلى التشفير ما بعد الكم، من حيث كيفية تفاعل المعدّات الحاسوبية والبرمجيات مع التشفير. يحتاج المخَطِّطون والجهات المُنَفِّذَة بشكلٍ عام إلى النظر في كيفية إجراء الانتقال القادم، مهما كان، بطريقة تشبه استبدال النظام الحالي ببديلٍ مطابق. ومع ذلك، نتوقّع أن يكون في الغالب أصلا أولئك المكلّفون بالتخطيط للأمن وتطبيقه على درايةٍ بهذه القضايا، ولكن يجب أولاً أن تكون القيادة التنظيمية الأخرى ومراقبي الموازنة على قناعةٍ بالفوائد المحتملة والفرصة التي يتيحها التفكير الاستراتيجي الطويل الأجل بشأن الأمن في سياق هذا الانتقال المُحدَّد. ولذلك، يجب التطرّق لضرورة إجراء هذه التغييرات في كلّ منظمة.

التوليف

إنّ السيناريو الأكثر ترجيحاً، نظراً للمعلومات الحالية ورأي الخبراء حول التقدُّم المحرَز في مجال تطوير الحواسيب الكمومية، وتوحيد معايير التشفير ما بعد الكمّ (PQC)، وأنماط الاعتماد التاريخية، هو سيناريو يتمّ فيه تطوير حاسوب كمومي ذي صلة بالتشفير بعد عدّة أعوام من إصدار معيارٍ للتشفير ما بعد الكمّ. إذا تمّ استخدام متوسطات تقديرات الخبراء، قد يتمّ ابتكار حاسوب كمومي ذي صلة بالتشفير بعد عشرة أعوام تقريباً من إصدار مسودة لمعيار التشفير ما بعد

الكمّ، ما قد يشكّل سيناريو يشبه للغاية ذلك الذي تمّ تحديده للسيناريو رقم 3 في استنباطنا لآراء الخبراء.

ففي هذا السيناريو، من المرجّح جداً أن يتمّ تطوير حواسيب كمومية ذات صلة بالتشفير بعد أن نكون قد بدأنا بالانتقال إلى التشفير ما بعد الكمّ ولكن قبل إكمال هذا الانتقال. قد تبقى نقاط الضعف قائمة في أشكال متعدّدة. قد تتخلّف منظمات متعدّدة في الانتقال إلى التشفير ما بعد الكم، بحيث لا تمنح الأولوية للتشفير ما بعد الكمّ في إدارة أمن دورة حياتها أو في منتجات الأمن الجديدة التي تشتريها. وقد تحتفظ على الأرجح تلك التي بدأت بالانتقال بنقاط ضعف في الأنظمة أو المكونات أو التطبيقات التي أهملت نقلها إلى التشفير الجديد. بشكلٍ أكثر عموماً، من المرجّح أن تبقى المعايير القديمة قيد الاستخدام لضمان قابلية التشغيل المتبادل حتى انتهاء الانتقال. قد تحتفظ المنتجات والأنظمة الطويلة الأجل التي يكون استبدالها باهظ الثمن وتحديثها صعباً بتشفيرٍ ضعيفٍ لأعوام عدّة وربما لعقود. أخيراً، ستواجه تلك المنظمات التي تمتلك معلومات حسّاسة يجب أن تبقى سريّة لأعوام أو عقود، وخاصةً تلك التي قد تُعتبر هدفاً عالي القيمة بالنسبة لأول مستخدمي الحاسوب الكمومي ذي صلة بالتشفير المرجّحين، عواقب ناتجة عن اتصالات تم التقاطها قبل الانتقال إلى التشفير ما بعد الكمّ ليجري فك تشفيرها بواسطة حاسوب كمومي. سيكون هذا الخطر أكبر بالنسبة إلى المنظمات التي انْتَظَرَت لفترة أطول للانتقال إلى التشفير ما بعد الكمّ. فقد تؤدّي نقاط الضعف هذه مجتمعةً إلى توقُّع مخاطر إضافيّة وكبيرة على الأمن الإلكتروني في المستقبل البعيد، حتى في هذا السيناريو المرجّح.

لحسن الحظ، يمكن التخفيف من الخطر الإجمالي عن طريق اتخاذ إجراءات استباقية لإعداد بنية اتصالاتنا التحتية لمواجهة الحواسيب الكمومية ومن خلال وضْع سياسات وضوابط لإدارة المخاطر قد تستطيع استغلال المحدوديات المرجّحة لقدرة الحواسيب الكمومية ذات الصلة المبكرة بالتشفير، على حدّ سواء. قد تترك لنا المهلة الزمنيّة الطويلة في السيناريو المرجّح، حيث يتمّ إصدار معيار التشفير ما بعد الكمّ بدون أن يكون قد تمّ تطوير الحواسيب الكمومية ذات الصلة بالتشفير بعد، فرصة لاتخاذ هذه الإجراءات الاستباقية.

سيتطلب التخفيف من المخاطر الناجمة عن الحوسبة الكمومية والتي تعترض بنية اتصالاتنا التحتية قيادة، وتنسيقاً، ورقابة مستدامة من جانِب سلطتي الحكومة الفيدراليّة التنفيذية والتشريعية، تبدأ فوراً وتستمرّ لفترة طويلة بعد تطوير الحواسيب الكمومية ذات الصلة بالتشفير. يجب النظر إلى الحوسبة الكمومية على أنّها تهديد أمني ملحّ، ويجب أن تحظى التدابير التحضيرية بالأولوية على المستوى الوطني. وعلى وجْه الخصوص، ينبغي على القادة والمنظمات الوطنية النظر في الخط الفاصل غير الواضح بين المنظمات المرتبطة بالأمن القومي وغير القومي. لا يزال باستطاعة المهاجمين الساعين وراء أهداف أقلّ حصانةً تُعنى بوظائف أساسيّة مثل معالجة عمليات الدفع وإدارة السجلات أن يتسبّبوا بأعطال وأضرارٍ كبيرةٍ بالأمن القومي إذا كانت غير محميّة، ويجب أن تُعطى الأولوية المناسبة في جهود الاستعداد الوطنية. علاوةً على ذلك، يجب إعطاء الأولوية لتطبيق التشفير ما بعد الكمّ في عملية تبادُل المفاتيح المرتبطة بالأهداف الحساسة في أقرب وقت ممكن عملياً للتخفيف من الخطر الناجم عن الاتصالات المشفرة المُلتقطة، مع السماح بالتشفير ما بعد الكمّ للمصادقة في وقت لاحق. في الرسائل، يجب تجنُّب التصريحات التخويفيّة غير الضروريّة بينما يتمّ تعزيز تقييم المخاطر والتخفيف منها بشكلٍ واقعي.

وأخيراً، يجب أن تستمر الجهود الرامية إلى تعزيز علوم وتكنولوجيا المعلومات الكمومية والاستثمار فيها، وبالتحديد الحوسبة الكمومية، حيث أنه يُرجّح، بمجرد توافُر التشفير ما بعد الكمّ، أن يُنظر إلى الحوسبة الكمومية على أنّها تشكّل أولاً فرصة لتحقيق تقدُّمٍ تكنولوجيٍّ كبيرٍ بدلاً من أن يُنظر إليها على أنّها خطرٌ أمنيٌّ.

الخُلاصة

يمثّل تطوير الحواسيب الكمومية ذات الصلة بالتشفير تهديداً لأمن بنية اتصالاتنا التحتية. يختلف هذا التهديد الأمني عن عددٍ من تهديدات الأمن الإلكتروني التي نواجهها اليوم والتي يجِد فيها مهاجمٌ ذكيٌّ طرقاً لتجاوُز أنظمة التشفير الهادفة إلى حماية المعلومات؛ بدلاً من ذلك، سيستخدِم المهاجِم جهازاً يقوم بضرب أنظمة التشفير تلك مباشرة، مخترقاً بذلك ركيزةً لأمن المعلومات. تُعتبر هذه القضية الأمنية كبيرة وملحّة، وقد تكون عواقب عدم التصرف لإيجاد حلولٍ لها مدمِّرة. من المتوقَّع أن تكون خوارزميات التشفير ما بعد الكمّ (PQC) فعالة في الدفاع في وجْه هجمات الحواسيب الكمومية، ولكن شرط أن يتمّ تطبيقها بقوة في الوقت المناسب.

من غير المتوقع أن يتمّ تطوير الحواسيب الكمومية ذات الصلة بالتشفير قبل 15 عاماً، على الرغم من تقدير الخبراء بأنّ ذلك الجدول الزمني غير مؤكّد للغاية، وقد تظهر الحواسيب الكمومية في وقت أقرب أو متأخّر جدّاً. سيكون الانتقال إلى التشفير ما بعد الكمّ محفوفاً بالتحديات وطويلاً، ولكن، من المحتمل أن يتركنا مع نقاط ضعف كبيرة حتى لو لم يتمّ تطوير الحواسيب ذات الصلة بالتشفير لعقود. إذا تصرّفنا في الوقت المناسب ومن خلال وضْع سياسات ملائمة، واتخاذ إجراءات للحد من المخاطر، وبحِسٍّ جَماعيٍّ للاستعداد للتهديد، عندئذٍ تتوفّر لنا فرصة لبناء بنية تحتية

مستقبلية للاتصالات تضمن الدرجة نفسها من الأمان أو تكون أكثر أماناً من الوضع القائم، على الرغم من تداخُل التهديدات الإلكترونية الناجمة عن الحواسيب التقليدية والكمومية. علاوةً على ذلك، قد نتمكّن من السعي وراء الحوسبة الكمومية على أنّها ببساطة قدرة حاسوبية جديدة تأسيسية، مع كلّ الفرص والوعود المرتبطة بها التي توفّرها للمجتمع، من دون خوف من التهديد المصاحب. وكما قال أحد الخبراء الذين قابلناهم، "يحتاج الناس إلى حلّ المشكلة والعمل عليها بجهد فحسب، وعلينا توفير التمويل لهم، وبعد ذلك يمكننا التركيز على استخدام حاسوب كمومي بالفعل لمساعدة البشرية بدلاً من تدمير العالَم. ... إنني غير مهتمٍّ بتدمير الإنترنت. إذا وجد[نا] حلولاً للمشكلة، هناك أمور عدّة أخرى يمكننا القيام بها باستخدام حاسوب كمومي." تملك الولايات المتحدة الحلول والوسائل، وعلى الأرجح الوقت الكافي، لتجنُّب أسوأ عواقب الحوسبة الكمومية، ولكن فقط إذا بدأت الآن في الاستعداد وبدرجة الاستعجال الملائمة.

الملحق A: النتائج التفصيلية

نتائج المقابلات

الجدول الزمني المُقدّر لظهور الحوسبة الكمومية

لقد طلبنا من الخبراء تقديم أفضل تقديراتهم لتاريخ ظهور حاسوبٍ كموميٍّ ذي صلة بالتشفير بالإضافة إلى أقرب عام وأبعد عام قد يحدث فيهما هذا الأمر. يبيّن الشكل A.1 نتائج كلّ مقابلة من المقابلات الخمس عشرة التي أجريناها ويَعرض المتوسّط المُرَجَّح بالاستناد إلى الخبرة في مجمل أحكام الخبراء.[20] في حال عدم عرْض أي تقديرات، يعني هذا أنّ الخبراء قد رفضوا تقديم التقديرات. يتمّ عرْض الأعوام على المحور العمودي، بينما يتمّ ترقيم المحور الأفقي من 1 إلى 15 مطابقةً للمقابلات الخمس عشرة التي أجريناها.[21]

اعتبَرَ خبيرٌ واحدٌ فقط أنّ العام 2022 هو أقرب تقديرٍ للتاريخ الذي سيتمّ فيه تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير، وفسَّر ذلك قائلاً:

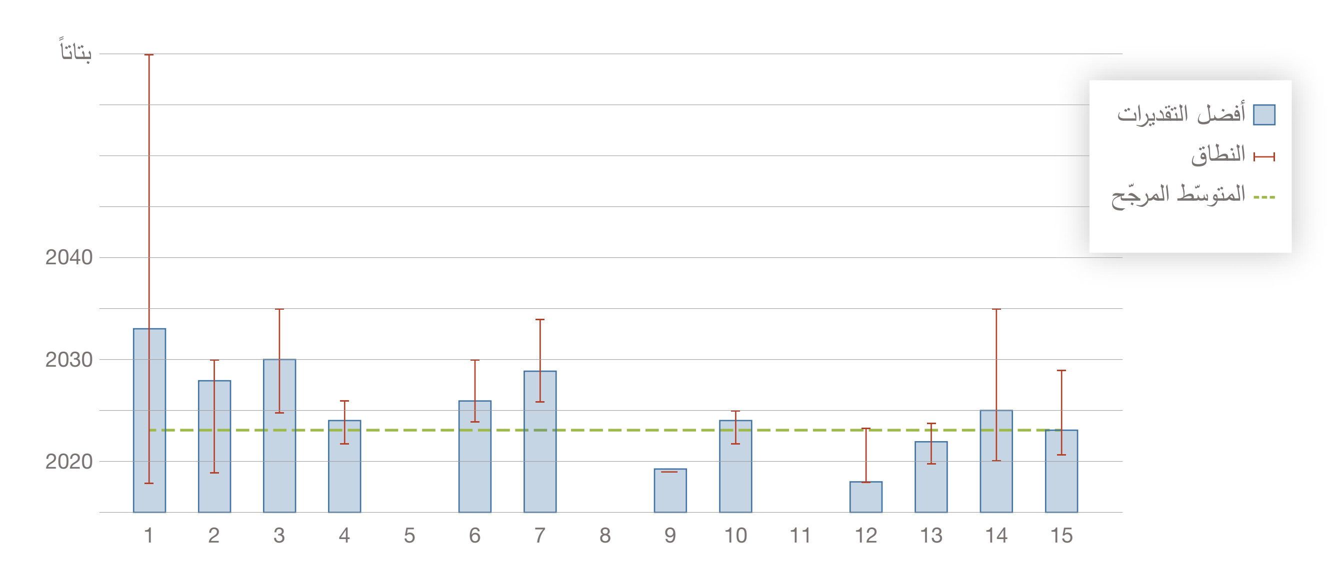
> إنك تحتاج أوّلاً إلى خوارزمية تصحيح الخطأ القابل للتوسّع. ... انظُر، إذا أرد[نا] وضْع 10,000 بتّة كموميّة على رقاقة، يمكن[نا] القيام بذلك. ولكن[نا] لا نفعل ذلك لأنها ليست جيّدة بعد. ... لم يتم اكتشاف تكنولوجيا [قابلية التوسّع] حتى الآن لأنّنا لم نصطدم بعد بطريق مسدود. ... قد يكون [العام 2022] غير مرجّح إلى حدٍّ كبير ولكنه ليس مستبعَداً تماماً. ... هناك دائماً فرصة لأن يكون بعض الجهات الفاعلة الحكوميّة متقدّماً قليلاً في هذا المجال. ... قد أتفاجأ، لكنّ ذلك قد لا يخلّ تماماً بتصوّري للواقع.

واعتَبَر خمسة خبراء آخرون أنّ العام 2023 هو أقرب عام ممكن. في المقابل، قال ما يقارب نصف الخبراء إنّه لا يزال من الممكن ألّا يتمّ تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير البتة. من المعروف أنّ جيل كالاي (Gil Kalai) يتبنى هذا الرأي، وهو أستاذ في معهد الرياضيات في الجامعة العبرية في القدس (Hebrew University of Jerusalem). فقد جادل كالاي بأنه، من منظور التعقيد الحسابي، ومن حيث قضية الضوضاء بشكلٍ أساسي، سينطوي حتماً الاحتفاظ بالبتات الكمومية في تراكبات حساسة للغاية على عيوبٍ بسبب أي تفاعل مع العالَم الخارجي. ويقول كالاي إن الحد من الضوضاء قد ينتهك بعض النظريات الحسابيّة الأساسية (موسكفيتش [Moskvitch]، 2018). وبالمثل، قال أحد خبرائنا، "إذا استمَعْتَ إلى بعض المشفرين، سيخبرونك أنّ الانصهار البارد سيحدث قبل أن تحصل على حاسوب كمومي." ويضيف خبيرٌ آخر، "[يمكن أن] يتبيّن ... أنّه لا يمكننا ربط عدد كافٍ من البتّات الكموميّة معاً بغضّ النظر عن التكنولوجيا المُعتمَدة؛ وأنّه على الرغم من كلّ العمل الذي يقومون به على هذه ... البتّات الكموميّة، لا يمكنهم العثور على مجالٍ من قِيَم المعلمات المحتملة لأنظمتهم المادية لتحقيق ذلك العمل."

استناداً إلى الخبرة، يُعتبر العام 2033 التقدير المتوسّط الأفضل للعام الذي يتم فيه ابتكار حاسوبٍ كموميٍّ ذي صلة

الشكل A.1

أفضل التقديرات والنطاق والمتوسّط المرجّح بالاستناد إلى الخبرة للجدول الزمني لتطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير



بالتشفير، أي بعد 15 عاماً من تاريخ إجراء المقابلة، وهو العام 2018. يتسق هذا التقدير مع تقديرات الدراسات السابقة المختلفة المذكورة أعلاه والتي تتنبأ بتواريخ مُرَجَّحَة تصادف منتصف ثلاثينيات القرن الواحد والعشرين. في حين لم يُقدِّر أيّ من خبرائنا بالضبط حدوث ذلك في العام 2033، قدّرَ بعضهم حصوله في العام 2032. وقال أحد هؤلاء،

> ثمّة عناصر كثيرة يجب معالجتها في هذا الإطار، ولكن بشكل تقريبيّ، إذا حَصَلتَ على البتّات الكموميّة القابلة للتوسّع بحلول عام 2022، [سيستغرق الأمر عشرة أعوام أخرى] لاعتبار أنك ستوسِّع نطاقها بحيث تشكِّل تهديداً [لاختراق التشفير باستخدام المفتاح العام، أو خوارزمية ريفست – شامير – أدلمان [Rivest–Shamir–Adleman (RSA)]. علاوةً على ذلك، ما زلنا نعمل على الخوارزميات. لا يصل عدد البتّات الكمومية الماديّة إلى نصف مليار أو مليار مثلما قدّرها الناس، ... ولكننا نعمل على النظرية لإيجاد حلّ لذلك ربّما.

كان الخبراء التابعون لصناعات القطاع الخاص أكثر تفاؤلاً من نظرائهم الأكاديميين بالنسبة إلى الجدول الزمني لتطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير. فغالباً ما أفاد الخبراء الأكاديميون بأن تطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير قد لا يتحقّق بتاتاً. وأفاد الخبراء الأكاديميون بأن العام 2035 هو أفضل تقدير لديهم، بينما أفاد خبراء القطاع الخاص بأن العام 2031 هو أفضل تقدير لديهم.

الجدول الزمني المقدّر لظهور التشفير ما بعد الكم

لقد طلبنا من الخبراء تقديم أفضل تقديراتهم لتاريخ ظهور مجموعة خوارزميات أمان كاملة تكون آمنة في وجْه هجومٍ كموميٍّ باستخدام أساليب التشفير باستخدام المفتاح العام ما بعد الكمّ بالإضافة إلى تقديراتهم بالنسبة إلى العام الأقرب والعام الأبعد اللذين قد يحدث فيهما هذا الأمر. هناك خوارزميات فاعلة موجودة حالياً لتطبيقات وأنظمة مختارة، غير أنّ قابلية التشغيل المتبادل والاعتماد على نطاقٍ واسع لن يكونا مجديين حتى يتمّ إصدار معيارٍ ما. يعمل المعهد الوطني للمعايير والتكنولوجيا (NIST) على وضْع معيارٍ يُفترض أن يتمّ إكماله بين عاميْ 2022 و2024، ولكن الأمر غير مضمون.

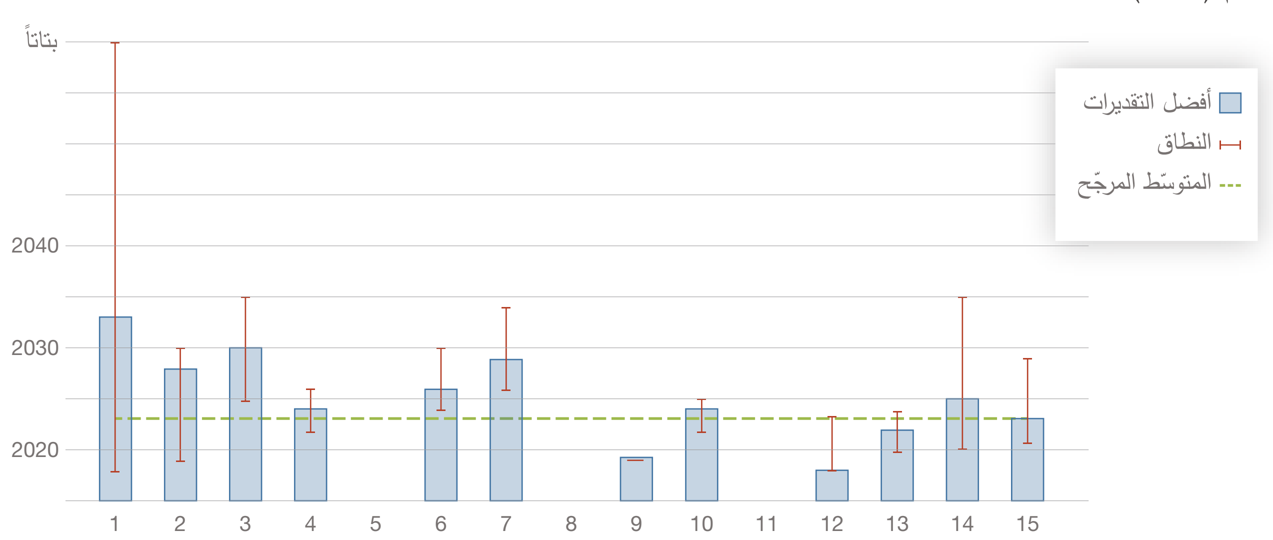
يبيّن الشكل A.2 النطاق وأفضل التقديرات للجدول الزمني للتشفير ما بعد الكمّ (PQC) في كلّ مقابلة من المقابلات الخمس عشرة التي أجريناها بالإضافة إلى المتوسط المرجّح بالاستناد إلى الخبرة في مجمل أحكام الخبراء. في حال عدم عرْض أي تقديرات، يعني هذا أنّ الخبراء قد رفضوا تقديم التقديرات. يتمّ عرْض الأعوام على المحور العمودي، بينما يعكس المحور الأفقي المقابلات الخمس عشرة التي أجريناها.

لقد قدَّر خبيران أنّ العام 2018 هو أقرب تاريخ قد يتمّ فيه ابتكار مجموعة خوارزميات أمان التشفير ما بعد الكمّ. وفسّر أحدهم الأمر على النحو الآتي:

> من الناحية التقنية، لديـ[نا] هذا حالياً. ... لديـ[نا] تجهيزات يمكنـ[نا] نشْرها اليوم لكلّ من التشفير باستخدام المفتاح العام والتوقيع الرقمي. إنها قابلة للاستخدام. إنها عمليّة، واستخدمناها في عروض تجريبيّة.

الشكل A.2

أفضل التقديرات والنطاق والمتوسّط المرجّح بالاستناد إلى الخبرة للجدول الزمني لابتكار مجموعة خوارزميات أمان التشفير ما بعد الكمّ (PQC)



عند الطرف الآخر من الطيف، قال أحد الخبراء إنّه من الممكن ألّا يتمّ تطوير مجموعة خوارزميات أمان تكون آمنة في وجْه هجومٍ كموميٍّ بتاتاً:

> إنك تعتقد أنّ مجموعة خوارزميات أمان هي آمنة في وجْه هجومٍ كموميٍّ إلى أن يتمّ اختراقها. [لذا]، فمن غير الممكن مرّةً أخرى تحديد [أبعد] عام، لأنّه ... بعد 30 أو 40 عاماً، يكتشف شخصٌ ما كيفية اختراقها.

بشكلٍ عام، اعتَقَد الخبراء أنّ تطوير التشفير ما بعد الكمّ قد يتمّ وفقاً لجدول المعهد الوطني للمعايير والتكنولوجيا. استناداً إلى الخبرة، اعتُبر العام 2023 التقدير المتوسط الأفضل للعام الذي يتم فيه ابتكار مجموعة خوارزميات أمان التشفير ما بعد الكمّ. على عكْس جدول الحوسبة الكمومية الزمني، لم تختلف الآراء حول ابتكار مجموعة خوارزميات أمان التشفير ما بعد الكمّ بحسب خلفية الخبراء. إنّ تقدير الخبراء الأكاديميين للمتوسّط المرجّح بالاستناد إلى الخبرة هو العام 2023، في حين أنّ تقدير خبراء القطاع الخاص للمتوسّط المرجّح بالاستناد إلى الخبرة هو العام 2024 — أي قبل عقْدٍ تقريباً من متوسط تقدير تطوير حاسوبٍ كموميّ.

الجدول الزمني المقدَّر لاعتماد التشفير ما بعد الكم

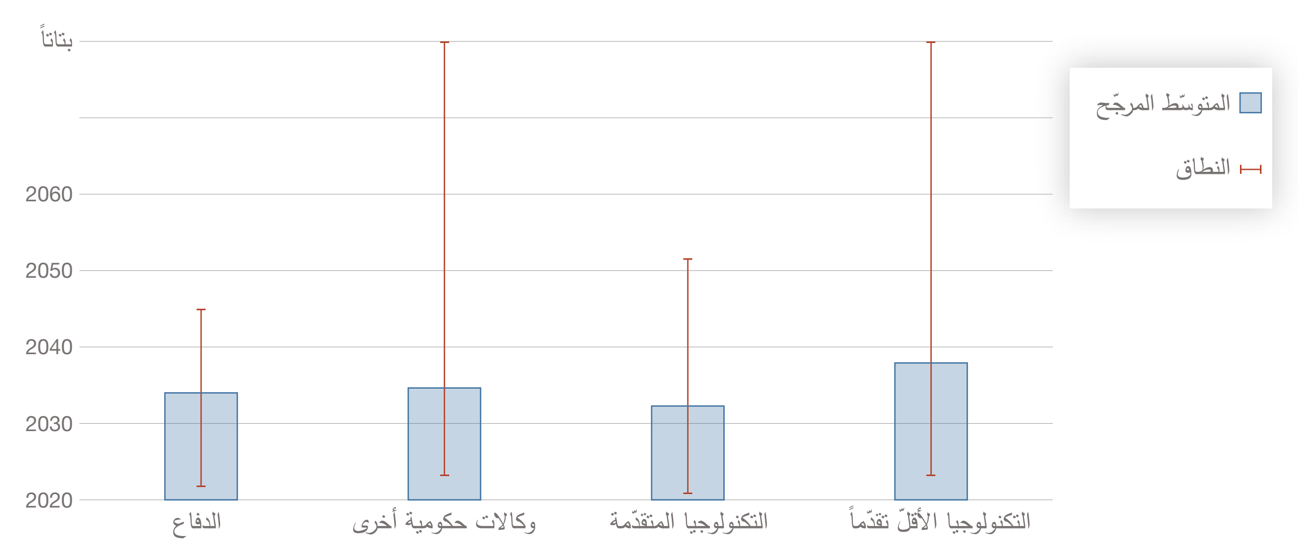
بما أنّ خوارزميات فاعلة موجودة حاليّاً، وأنّه من المقرّر أن يستكمل المعهد الوطني للمعايير والتكنولوجيا (NIST) معياراً بين عاميْ 2022 و2024، تكمن القضية الأساسيّة في تحديد تاريخ وكيفية اعتماد التشفير ما بعد الكمّ (PQC).

لقد طلبنا من الخبراء تقديم أفضل تقديراتهم لتاريخ الاعتماد وعرّفنا الاعتماد بأنه "اعتماد [القطاع] التشفير ما بعد الكمّ في أمن [القطاع] بنسبة تفوق 95 في المئة." وطلبنا منهم أيضاً تقديم تقديراتهم بالنسبة إلى العام الأقرب والعام الأبعد للاعتماد في قطاعات مختلفة: قاعدة الدفاع والاستخبارات الأمريكية (U.S. defense and intelligence base)، والوكالات الحكومية الأمريكية الأخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص (على وجه التحديد، خدمات المعلومات، والخدمات المالية، وصناعات الدفاع غير الحكومية)، وصناعات التكنولوجيا الأقلّ تقدّماً في القطاع الخاص (على وجه التحديد، الاتصالات، والرعاية الصحية، والتصنيع). من الواضح أنّ هذه التصنيفات العامّة قد تسيء تمثيل الوضع التكنولوجي في شركات متعدّدة تقع ضمن إحدى المجموعتين (على سبيل المثال، قد تكون بعض شركات الخدمات المالية أقل تقدُّماً من الناحية التكنولوجية، وقد تكون بعض شركات الاتصالات في الطليعة من حيث اعتماد التشفير ما بعد الكمّ)، لكنها اعتُبِرَت تحديداً بديهياً ومفيداً اتّفق الخبراء بشكلٍ عام على أنّه توضيحيّ.

يبيّن الشكل A.3 التقديرات الإجمالية لكلّ قطاع: المتوسطات المرجّحة بالاستناد إلى الخبرة والنطاق الكامل (أقرب عام في التقديرات وأبعد عام في التقديرات). كما في الأشكال السابقة، يتمّ عرْض الأعوام على المحور العمودي، بينما يعكس المحور الأفقي القطاعات.

الشكل A.3

المتوسّط المرجّح بالاستناد إلى الخبرة والنطاق بحسب جميع الخبراء بالنسبة إلى الجدول الزمني لاعتماد التشفير ما بعد الكمّ (PQC) في قاعدة الدفاع والاستخبارات الأمريكية (U.S. defense and intelligence base)، والوكالات الحكومية الأمريكية الأخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، وصناعات التكنولوجيا الأقلّ تقدُّماً في القطاع الخاص



يعتقد الخبراء أنّ قاعدة الدفاع والاستخبارات الأمريكية وصناعات التكنولوجيا المتقدّمة في القطاع الخاص ستسارع في اعتماد التشفير ما بعد الكمّ. بالنسبة إلى الوكالات الحكومية الأمريكية الأخرى وصناعات التكنولوجيا الأقل تقدُّماً، يعتقد الخبراء أنّ الاعتماد سيتمّ بوقتٍ لاحقٍ وقد لا يجري بتاتاً. أمّا بالنسبة إلى قاعدة الدفاع والاستخبارات الأمريكية وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، فإنّ التقديرات الأقرب هي عاميْ 2021 و2022. وفي سياق وصْف الاستدلال الذي أدّى إلى تقدير العام 2018، ذَكر أحد الخبراء أنّ هذا الاستدلال يفترض استخدام حلول التشفير ما بعد الكمّ غير الموحّدة المتوفّرة حالياً واستخدام "دورة اعتماد مكثّفة." في حين قد تجِد منظمات صناعات التكنولوجيا المتقدّمة في القطاع الخاص سهولة أكبر في اعتماد التشفير ما بعد الكمّ الجديد لأنّ "عدد الأنظمة الموروثة لديها أقل، و[إنّه] من الأسهل تحسين البنية التحتية، [و] يمكنك فرْض الرُقع (التصحيحات) على عددٍ أكبر من الأشخاص،" سيكون الاعتماد بالنسبة إلى قاعدة الدفاع والاستخبارات الأمريكية سريعاً لأنّ الحاجة إليه كبيرة للغاية.

يعود بعض الاختلاف إلى اتساع نطاق التعريفات القطاعية. ففي حين أنّ تعريف قاعدة الدفاع والاستخبارات الأمريكية ضيّق نسبيّاً، من الممكن أن يشمل كلّ قطاع من القطاعات الأخرى مجموعة متنوعة من المنظمات. فقد قال أحد الخبراء إنّ الوكالات الحكومية الأمريكية الأخرى (التي تشمل الوكالات الحكومية والمحلية والفيدرالية) قد لا تعتمد التشفير ما بعد الكمّ بتاتاً إن لم يُفرَض ذلك عليها. وستعتمد عدّة منظّمات في مجال التكنولوجيا المتقدّمة التشفير ما بعد الكمّ بسرعة، ولكن قد تكون حاجة بعض المنظمات أقلّ إلحاحاً أو قد يواجه هذا البعض قيوداً مالية ملحّة وبالتالي يكون أقلّ سرعةً في الاعتماد. قد تركّز الشركات الصغيرة بشكلٍ خاص على شحْن المنتجات في الوقت المحدّد وحسب وبالتالي قد تركّز أقل على اعتماد أفضل مستوى أمن. تاريخياً، كانت منظّمات صناعات التكنولوجيا الأقل تقدُماً بطيئة في اعتماد معايير الأمن الإلكتروني الجديدة، ولا يزال عدد كبير منها يملك أنظمة موروثة ذات أمن قديم، لذلك فإنها قد تتبع الأنماط التاريخية إذا لم يقُم بعضها بالاعتماد بتاتاً.

السيناريوهات

طلبنا من الخبراء النظر في ثلاثة سيناريوهات افتراضية، وهي:

1. يتمّ ابتكار حاسوبٍ كمّوميٍّ ذي صلة بالتشفير قبل توحيد معايير التشفير ما بعد الكمّ (PQC)
2. يتمّ ابتكار حاسوبٍ كمّوميٍّ ذي صلة بالتشفير عند الاعتماد أو بمجرّد البدء باعتماد معايير التشفير ما بعد الكمّ (PQC) الموحّدة حديثاً
3. يتمّ ابتكار حاسوبٍ كمّوميٍّ ذي صلة بالتشفير بعد عشرة أعوام من توحيد معايير التشفير ما بعد الكمّ (PQC).

طُلب من الخبراء تقييم عواقب كلّ سيناريو بالنسبة إلى قاعدة الدفاع والاستخبارات الأمريكية، والوكالات الحكومية الأمريكية الأخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، وصناعات التكنولوجيا الأقل تقدُّماً في القطاع الخاص، مع افتراض أنّه لم يتمّ اتخاذ أي إجراءات إضافية لمعالجة أي نقطة ضعف أمنية تسبّبها الحواسيب الكمومية عدا الاعتماد النهائي للتشفير ما بعد الكمّ.

بالنسبة إلى كلّ سيناريو وقطاع، قدّم الخبراء توزيعاً للاحتمالات على ثلاثة مستويات من العواقب. اعتَبر المستوى الأول أنّ الجهات الفاعلة الخبيثة قادرة أحياناً على الحصول على معلومات حسّاسة. واعتَبر المستوى الثاني أنّ الجهات الفاعلة الخبيثة قادرة في كثير من الأحيان على الوصول إلى المعلومات الحساسة. في حين اعتَبر المستوى الثالث أنّ الجهات الفاعلة الخبيثة سيطرت بالكامل على أنظمة المعلومات. كان المطلوب أن يصل مجموع الاحتمالات المُفاد بها إلى 100 لكلّ سيناريو وقطاع. مثلاً، بالنسبة إلى منظمة الدفاع والاستخبارات الأمريكية بموجب السيناريو رقم 1، قد يفيد الخبراء بأنّهم يتوقّعون أن تحصل الجهات الفاعلة الخبيثة على معلومات حساسة أحياناً بنسبة 60 في المئة من الوقت، والوصول إلى المعلومات الحساسة في كثير من الأحيان بنسبة 30 في المئة من الوقت، والسيطرة الكاملة على أنظمة المعلومات بنسبة 10 في المئة من الوقت. وفي حال لم يصل مجموع احتمالات الخبراء إلى 100، طلبنا منهم مراجعة تقديراتهم.

باستخدام الاحتمالات المُفاد بها، نستخلص درجة (score) تعكُس حجم العواقب استناداً إلى تصنيفٍ ترتيبي ومتساوٍ للعواقب. اعتَبِر أنّ p_1، p_2، p_3 ترمز إلى الاحتمالات التي أفاد بها الخبراء عن كلّ مستوى من مستويات العواقب الثلاثة، واعتَبِر أنّ v_1، v_2، v_3 ترمز إلى القِيَم المرتبطة بمستويات العواقب الثلاثة. إنّنا نحدِّد أيضاً علاقة بسيطة بين قِيَم مستويات العواقب الثلاثة، وبالتحديد أنّ $v_2 = 2v_1$ و $v_3 = 3v_1$. فاستخرجنا الدرجات باستخدام المعادلة التالية:

$$Score = \sum_{c=1}^{3} v_c p_c.$$

ومن أجل احتساب الدرجات باستخدام هذه المعادلة والعلاقات المحدَّدة، كلّ ما هو مطلوب هو اختيار قيمة لـِ v_1. يمكن اختيار أي قيمة لـv_1؛ فهي ببساطة توفِّر كمية أساسية للجميع لإجراء مقارنات كميّة نسبية بين العواقب. في الأشكال التالية، حدّدنا أنّ $v_1 = 25$، ونتيجةً لذلك، $v_2 = 50$، و$v_3 = 75$. ثم نحتسب درجات العواقب باستخدام الاحتمالات التي أفاد بها كلّ من الخبراء. بعد ذلك، مستخدمين التقييمات بالاستناد إلى الخبرة، نقوم بإنتاج متوسطات مرجّحة بالاستناد إلى الخبرة لتجميع النتائج. يبيّن الشكل A.4 هذه النتائج المجمّعة، ممّا يتيح المقارنة على امتداد السيناريوهات الثلاثة وكلّ من القطاعات.

تبيّن هذه النتائج، بشكلٍ غير مفاجئ، أنّه وبالنسبة إلى كلّ قطاع، سيُنتج السيناريو رقم 1 أكثر العواقب كارثيّة. ومع ذلك، لم يوافق جميع الخبراء على هذا الأمر. لقد اعتقَد البعض أنّه قد لا يكون هناك فرْق بين العواقب في إطار السيناريو رقم 1 والسيناريو رقم 2. ففي حين يتيح السيناريو رقم 2 بذْل جهود للاعتماد على مدار ثلاثة أعوام بعد توحيد معايير التشفير ما بعد الكمّ (PQC)، يكون "توحيد المعايير بمثابة طلقة البداية". كان نطاق الاعتماد الزمني الدافِع الرئيسي لهذا الرأي. وكما قال أحد الخبراء،

> سيقوم الأشخاص بشكلٍ محتملٍ بتطبيق خوارزميات مختلفة بتفاؤل قبل انتهاء عملية توحيد المعايير، ولكن من حيث إخضاع كلّ منها بالفعل لدورة اختبار المُنتَج وإصداره ووضْع وحدة معدات حاسوبية نمطية في برنامج التحقق من وحدة التشفير النمطية وكلّ تلك الأشياء، فهي لن تحدث إلى أن يتمّ توحيد المعايير فعلياً. ... من ثم هناك دورة شراء. ... لذلك أعتقِد أنّ ثلاثة أعوام ... هي المدّة الفعلية التي يحتاجها الأشخاص بشكلٍ أساسيٍّ لتشغيل أوّل نظام مُحدَّث على الإطلاق.

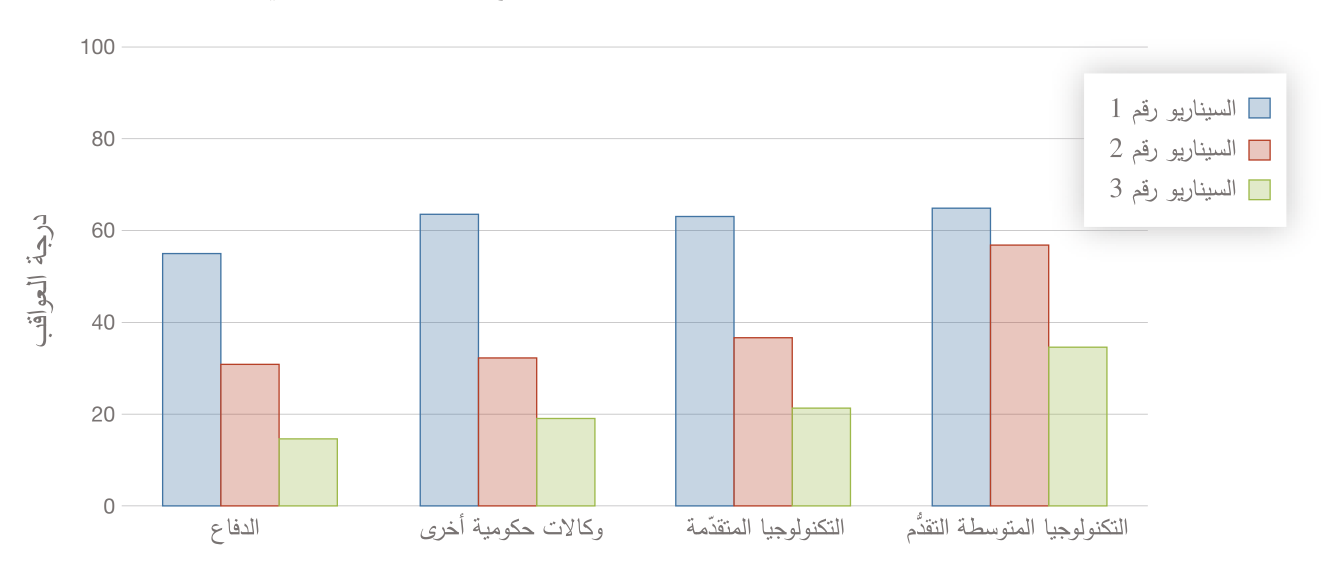
كما قد نتوقّعه، اعتبَر الخبراء عموماً أنّ عواقب السيناريو رقم 1 هي الأكثر خطورة. ويكمن الأمر الأكثر إثارةً للاهتمام في اعتقاد الخبراء بأنّ عواقب كلّ سيناريو ستكون أقلّ خطورةً في مؤسسة الدفاع والاستخبارات الأمريكية. ليست هذه النتيجة بديهية مسبقاً إذ تُعتبَر مؤسسة الدفاع والاستخبارات الأمريكية هدفاً عالي القيمة وواضحاً للجهات الفاعلة الخبيثة.

ومع ذلك، جادَل الخبراء بأنه أولاً، تدرك مؤسسة الدفاع والاستخبارات الأمريكية التهديد المحتمل وقد تَعَهَّدَت أصلاً بالعمل بشكلٍ استباقيٍّ ووقائيٍّ لمعالجة أي نقاط ضعف أمنية. وفي عام 2015، أعلنَت وكالة الأمن القومي (NSA) أنها كانت تخطط للانتقال إلى التشفير الآمن كمومياً، وأصْدَرَت قيادة أخرى في منظمات الأمن الإلكتروني داخل وزارة الدفاع (Department of Defense) تصريحات علانيّة تعترف فيها بالحاجة إلى الاستعداد لمواجهة التهديد الناجم عن الحوسبة الكمومية (فريدمان [Friedman]، 2018). ثانياً، اعتقَد الخبراء أنّ مؤسسة الدفاع والاستخبارات الأمريكية قد بَنَت استجابات آمنة عند التعطّل وإجراءات مضادة. وكما قال أحدهم،

> قد يحتاج [المهاجمون] إلى الوصول إلى البنى التحتية، المعزولة عن الشبكات غير الآمنة ... والتي يُفترض أيضاً أن يعتمد بعضها على التشفير الذي لا تتدرج

الشكل A.4

درجات المتوسّطات المرجّحة بالاستناد إلى الخبرة للعواقب المترتبة، بحسب القطاع، لكلّ سيناريو افتراضيّ



خصائصه في الملْك العام لأنه تمّ تطويرها في وضعيات سرية. بالإضافة إلى ذلك، ... إنّ قطاع الدفاع ... [يتمتّع] بالقدرة على التحوّل إلى آليات غير ضعيفة.

من غير المُرجّح أن تكون الإجراءات المضادة والاستجابات الآمنة عند التعطّل التي قد تعتمدها مؤسسة الدفاع والاستخبارات الأمريكية الحلّ الشافي ولكنها قد توفّر بعض الحماية. علاوةً على ذلك، تُعتبر هيكلية مؤسسة الدفاع والاستخبارات الأمريكية الهرمية التي تُيسِّر التنسيق وآخر سبيل للاتصال إحدى الاستجابات الآمنة عند التعطّل. وكما قال أحد الخبراء،

> في أسوأ الحالات، تمتلك وكالات الدفاع آلية ليست ربّما متاحة لمعظم المؤسسات التجارية، وبالتحديد باستطاعة [وزير الدفاع (Defense Secretary)] الظهور على التلفزيون والقول، "انتباه إلى جميع الوحدات، توقفوا عن استخدام قنوات الاتصال المشفرة المختلفة، وعوضاً عن ذلك قوموا بتعيين ملازمٍ ثانٍ من وحداتكم لنقل الوثائق على ورق في حقيبة."

ثالثاً، قد تكون الوكالات الحكومية غير الدفاعية وكيانات القطاع الخاص أكثر ضعفاً في وجْه هجومٍ مقارنةً بالوكالات الحكومية، لأنها تحتفظ ببيانات قيّمة جدّاً بالنسبة إلى المهاجمين ولكنّها قد تكون أقل حمايةً من معلومات الدفاع والاستخبارات السرية. وتحافظ وكالات أمريكية، مثل دائرة ضريبة الدخل (Internal Revenue Service) أو إدارة الضمان الاجتماعي (Social Security Administration)، على أنظمة موروثة قديمة ومتهالكة (مكتب المساءلة الحكومية [GAO]، 2016). قد تكون أيضاً أقل مرونةً في الرد على تهديدٍ متصوَّر:

> يكمن البديل بشكلٍ أساسيٍّ في مجرّد إيقاف كلّ شيء، وإنني أعتقِد أنّه في معظم الوكالات غير الدفاعية، لا يُعتبر ذلك خياراً متاحاً. لا شكّ في أنّه لم يكن باستطاعتك القيام بذلك في وزارة الطاقة (Department of Energy). قد لا يكون باستطاعتك القيام بذلك في أيّ من الوكالات الحكومية التي تُعنى بتوفير منافع اجتماعية، وإلّا قد تتسبّب باضطرابات أهلية هائلة. وبالتأكيد قد لا يكون باستطاعتك القيام بذلك في [الإدارة الفيدرالية للطيران (Federal Aviation Administration)]، وهَلُم جرّاً.

بالنسبة إلى التكنولوجيا الأقل تقدُّماً في القطاع الخاص، يعتقد الخبراء أنّ عواقب السيناريو رقم 1 ستكون الأسوأ، غير أنّ عواقب السيناريو رقم 2 لن تكون أقلّ خطورة. إنّ هذا مثيرٌ للاهتمام، لأنّه في السيناريو رقم 2، كان التشفير ما بعد الكمّ متاحاً لمدة ثلاثة أعوام قبل ظهور حاسوبٍ كموميٍّ ذي صلة بالتشفير. ولكن يبقى الاعتماد القضية الرئيسية. فلأسباب عدّة، من المرجح أن تعتمد المنظمات في صناعات التكنولوجيا الأقل تقدُّماً التشفير ما بعد الكمّ بسرعةٍ أقلّ. إنّ أحد الأسباب هو الوعي. نظراً لأنه من المرجح أن تستمد صناعات التكنولوجيا الأقل تقدُّماً قيمةً أقل من الحوسبة الكمومية، فمن المرجح أيضاً أن تكون أقل وعياً بالمخاطر. وأشار أحد الخبراء إلى أنّه على الرغم من الحاجة إلى اتخاذ تدبير فوري لاختبار حلول التشفير ما بعد الكمّ، "يمكنني أن أعدّ على أصابع يدي [عدد الشركات] التي تنشر أصلاً التشفير [ما بعد الكم]". فيؤدّي مستوى أدنى من الوعي بالمخاطر إلى تقليص أرجحية الاستثمار في التخفيف منها. وحتى عندما يكون مستوى الوعي مرتفعاً، لا تزال قيود مالية قائمة. إنّ التدابير المبكرة هي أكثر تكلفةً من التدابير اللاحقة لأنّ التكنولوجيا أحدث. ودائماً ما يتمّ احتساب الفوائد التي تترتب على الأمن بالمقارنة مع التكاليف.

سينطوي اعتماد التشفير ما بعد الكمّ في صناعات التكنولوجيا الأقل تقدُّماً على دورات المنتجات. من غير المرجّح أن تستثمر المنظمات العاملة في مجال صناعات التكنولوجيا الأقل تقدُّماً في حلول التشفير ما بعد الكمّ المطوَّرَة داخلياً. بدلاً من ذلك، ستشتري حلولاً جاهزة من الموردين. وهذا يعني أنّه سيتعين على مورديها أولاً تطوير الحلول واختبارها وإنتاجها وعرْضها للبيع. تعتمد كلّ منظمة أيضاً دورةً لتجديد الإمداد والتكنولوجيا. ولا يتم استبدال موارد الحوسبة في صناعات التكنولوجيا الأقل تقدُّماً كلّ عامٍ أو حتى كل بضعة أعوام. فهذا يعني أنّ الأمر سيستغرق وقتاً طويلاً أو سيتطلّب أموالاً إضافيةً لاستبدال موارد الحوسبة الحالية بمنتجات جديدة ضمَّنَت حلول التشفير ما بعد الكمّ.

أخيراً، اعتَقَد الخبراء أنّ عواقب كلّ سيناريو ستكون قابلة للمقارنة بين الوكالات الحكومية الأمريكية الأخرى وصناعات التكنولوجيا المتقدِّمة في القطاع الخاص. ويعود جزء من هذا التشابه إلى التجميع. فقد يتمّ تعريف كلّ قطاع من هذه القطاعات على نطاقٍ واسعٍ ويتضمن بعض الكيانات التي ستتّخِذ خطوات متعدّدة لضمان أمن المعلومات التي تحتفظ بها، بالإضافة إلى كيانات أخرى لن تتّخِذ خطوات كافية. بالإضافة إلى ذلك، في القطاعات التي لا تفرض عليها اللوائح التطبيق الاستباقي للإجراءات الأمنية الجديدة والمتقدمة، سيكون التطبيق بطيئاً بسبب ارتفاع التكلفة:

> حتى في جوجل (Google)، والتي أعتقِد أنّها ربّما الأفضل في هذا المجال، هناك كمٌّ هائلٌ من البنية

التحتية، وتتجاوز المرونة المطلوبة لضمان عدم قيام أي شخص بإجراء تحديث برمجيات تمّ توقيعها بشكلٍ خبيث، أو ما يشبه ذلك، الاحتياطات اليومية التي يتمّ تضمينها في الممارسات التجارية وبالتالي قد يتطلّب الأمر بذْل جهْدٍ استثنائيٍّ في سبيل ضمان سلامة الحاسوب لمنع حدوث ذلك بشكلٍ موثوق.

الدراسة الاستقصائية حول المستهلِكين

لقد استخدمنا دراسة استقصائية حول المستهلِكين لأنّ المخاطر التي تعترض التشفير والناجمة عن الحوسبة الكمومية تمتدّ إلى الاقتصاد العالمي الحديث. فإذا قلّلَ المستهلِكون من تواجدهم على الإنترنت أو أعادوا توجيهه خوفاً على أمن معلوماتهم الشخصية والمالية وغيرها من المعلومات الخاصة بهم التي تنطوي عليها التفاعلات الرقمية، قد يكون لذلك تأثيرات كبيرة، على كلّ من المنظمات التي لا تتخذ الخطوات الاحترازية اللازمة، وعلى الاقتصاد العالمي الحديث. وعلى العكس، قد تكون التأثيرات ضئيلة لأن المستهلِكين لا يولون إلّا القليل من القيمة لخصوصية معلوماتهم أو لا يملكون القوة على التحكُّم في خصوصيتهم.

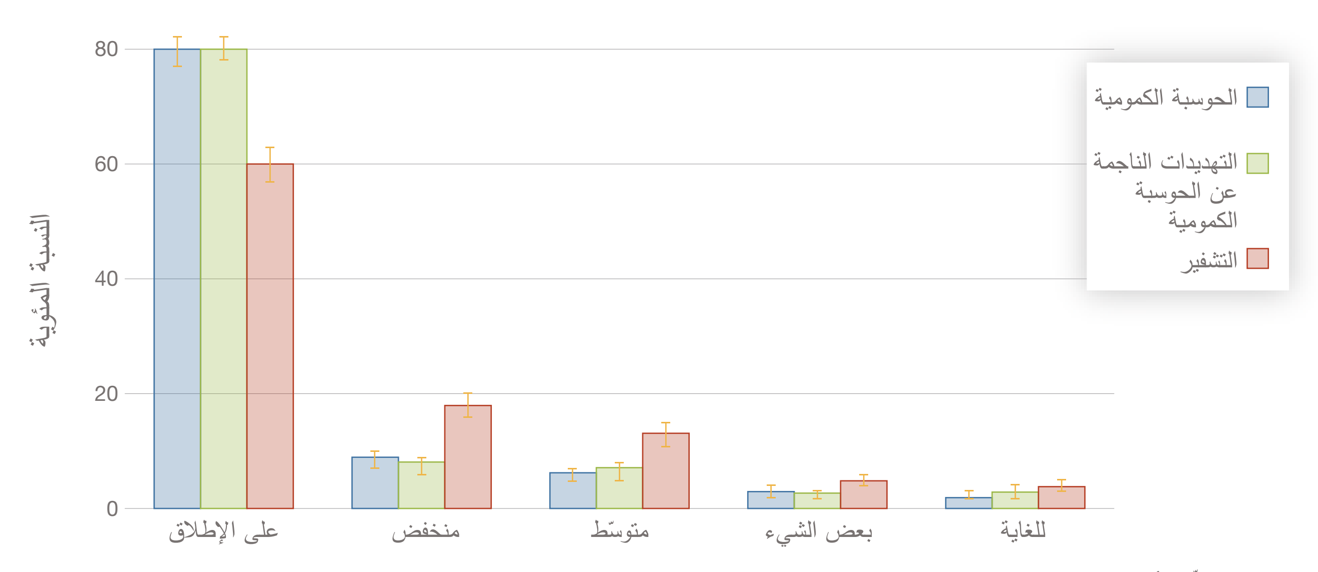
يتضمّن الملحق C تفاصيل الدراسة الاستقصائية حول المستهلِكين، بما في ذلك الأسئلة الدقيقة التي تمّ طرْحها، وهي متوفّرة على الموقع الإلكتروني: www.rand.org/pubs/research_reports/RR3102.html.

الوعي

لقد استخدمنا دراسة استقصائية حول المستهلِكين شَمَلَت 1,100 مجيب، كما تمّ وصْفها، لاستكشاف الوعي بالحوسبة الكمومية، وكيفية استخدام التشفير على الإنترنت، وكيفية تأثير الحوسبة الكمومية على الأمن الإلكتروني. كما هو موضح في الشكل A.5، أفاد حوالي 80 في المئة من المستهلِكين بأنّهم ليسوا على وعيٍ على الإطلاق بالحوسبة الكمومية أو بالتهديدات المحتملة التي قد تشكّلها على الأمن الإلكتروني. علاوةً على ذلك، فإنّ معظم الذين أفادوا ببعض الوعي لديهم مستوى وعي منخفض. يُعتبر الوعي بكيفية استخدام التشفير على الإنترنت أعلى نسبيّاً؛ ومع ذلك، أفادت غالبية المستهلِكين (60 في المئة) بأنها ليست على وعيٍ على الإطلاق بالتشفير على الإنترنت.

بحسب العمر، تُبيّن النتائج بشكلٍ غير مفاجئ أنّ مستوى الوعي بالحوسبة الكمومية أعلى بين أولئك الذين تتراوح أعمارهم بين 18 و34 عاماً، ولكن حتى بين هذه المجموعة لا يزال مستوى الوعي منخفضاً، في حين لا يعي 76 في المئة بالحوسبة الكمومية على الإطلاق. وفي الوقت عينه، فإن 81 في المئة من الأشخاص الذين تتراوح أعمارهم بين 35 و54 عاماً و82 في المئة من الأشخاص الذين يبلغون 55 عاماً من العمر فأكبر ليسوا على وعيٍ على الإطلاق بالحوسبة الكمومية. علاوةً على ذلك، حتّى بين المجيبين الأصغر سناً الذين شملتهم الدراسة الاستقصائية، كان مستوى الوعي بالتهديدات المحتملة الناجمة عن الحوسبة الكمومية منخفضاً بحيث أفادت نسبة 77 في المئة من

الشكل A.5
الوعي بالحوسبة الكمومية، والتشفير، والتهديدات التي تعترض التشفير والناجمة عن الحوسبة الكمومية



ملاحظة: تمثّل الأعمدة المتوسّط المرجّح؛ وتشير الخطوط الرفيعة إلى النطاق.

الأشخاص الذين تتراوح أعمارهم بين 18 و34 عاماً بأنها لم تكن على وعيٍ بها على الإطلاق. وكان الرجال أكثر أرجحية من النساء في الإفادة عن وعيٍ بالحوسبة الكمومية، وكيفية استخدام التشفير على الإنترنت، والتهديدات المحتملة التي تعترض التشفير والناجمة عن الحوسبة الكمومية.

عمليات اختراق الأمن الإلكتروني السابقة

نظراً لأنّ فهْم كيفية استجابة الأشخاص لحوادث الأمن الإلكتروني في الماضي يُعدّ أمراً أساسيّاً للتنبؤ بكيفية استجابتهم في المستقبل، بَحَثَت الدراسة الاستقصائية التي أجريناها في مواقف المستهلِكين إزاء عمليات الاختراق السابقة.

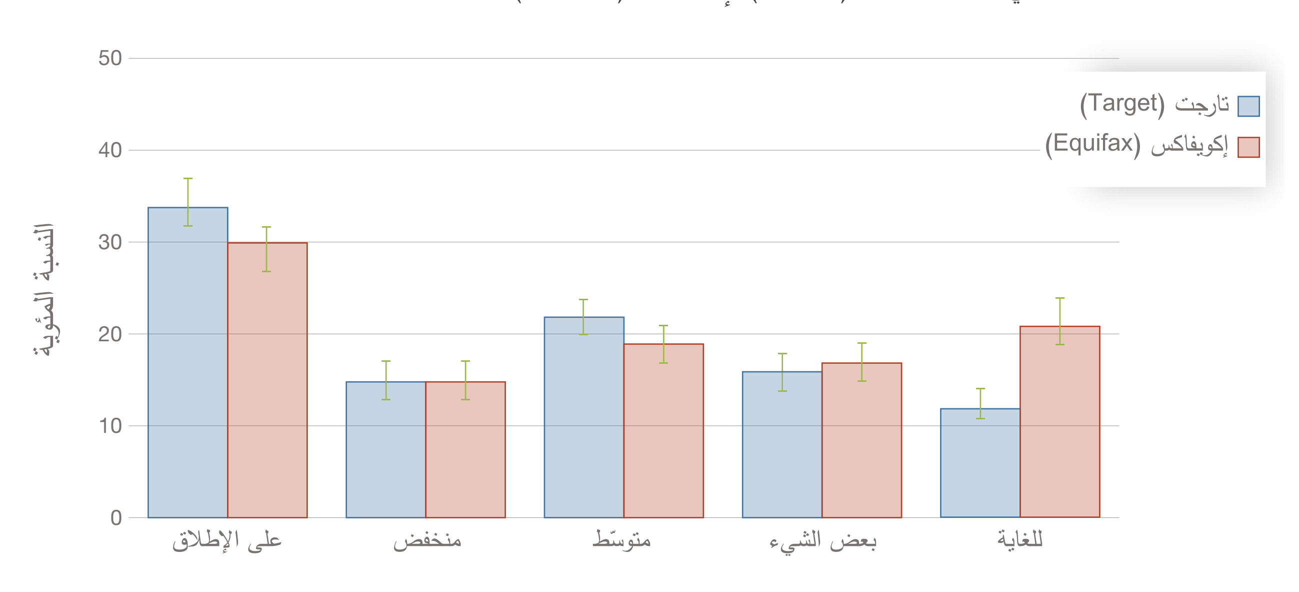
يبيّن الشكل A.6 مستوى القلق بشأن عملية اختراق تارجت (Target) عام 2013 وعملية اختراق إكويفاكس (Equifax) عام 2017. بالإجمال، كان مستوى القلق بشأن عمليتَي الاختراق متشابهاً، على الرغم من أنّ القلق إزاء عملية اختراق إكويفاكس كان أشدّ بقليل. ولأنّ إكويفاكس تجمع معلومات مالية حسّاسة حول جميع المقيمين في الولايات المتحدة، بينما تملك تارجت معلومات عن متسوّقيها فحسب، يجب منطقيّاً أن يكون مستوى القلق بشأن عملية اختراق إكويفاكس أكبرهما. لقد توافَقَت النتائج مع هذا التوقّع، حيث أفادت نسبة 66 في المئة بمستوى معيّن من القلق (من منخفض إلى شديد للغاية) بعد عملية اختراق تارجت عام 2013، وأفادت نسبة 70 في المئة عن قلق بعد عملية اختراق إكويفاكس. أفادت نسبة أكبر بأنّها "قلقة للغاية" بشأن عملية اختراق إكويفاكس (21 في المئة) أكثر منها بشأن عملية اختراق تارجت (12 في المئة). وبالنظر إلى الفرْق في كمية المعلومات الشخصية التي تحتفظ بها إكويفاكس وتارجت، تشير النتائج إلى أنّ المستهلِكين يفهمون الفرْق في العواقب بين حادثتي الأمن الإلكتروني.

في حين لا توجد أوجه فرْق كبيرة في مستوى القلق بحسب الجنس بعد وقوع هاتين الحادثتين المتعلّقتين بالأمن الإلكتروني، إلّا أنّ هناك أوجه فرْق كبيرة بحسب العمر ، حيث يشعر كبار السن بشكلٍ عام بقلقٍ أكبر بشأن حادثتَي الأمن الإلكتروني. يبيّن الجانب الأيسر من الشكل A.7 مستوى القلق بحسب العمر بشأن عملية اختراق تارجت، ويبيّن الجانب الأيمن مستوى القلق بحسب العمر بشأن عملية اختراق إكويفاكس. وضمن الفئة العمرية التي تتراوح بين 18 و34 عاماً، أعرَب ما يقارب 40 في المئة عن عدم قلق بشأن أيّ من عمليتَي الاختراق، ولكن في حين أعرَب 10 في المئة فقط عن قلقهم الشديد بشأن عملية اختراق تارجت، أعرَب 17 في المئة عن قلقهم الشديد بشأن عملية اختراق إكويفاكس. وأعرَب الأشخاص الذين يبلغون من العمر 55 عاماً فأكبر عن قلقٍ أشدّ للغاية مقارنةً بالفئات العمرية الأصغر سناً بشأن كلّ من عملية اختراق تارجت (17 في المئة مقابل 10 في المئة) وعملية اختراق إكويفاكس (27 في المئة مقابل 18 في المئة). وعلى الرغم من أنّ الأكثريّة (29 في المئة) في الفئة العمرية من 55 عاماً فأكبر لم تكن قلقة على الإطلاق بشأن عملية اختراق تارجت، كانت الأكثرية (27 في المئة) في الفئة العمرية من 55 عاماً فأكبر قلقة للغاية بشأن عملية اختراق إكويفاكس.

طلبنا أيضاً من المجيبين الإفادة بأي تدابير اتخذوها بعد عملية اختراق تارجت وعملية اختراق إكويفاكس. يبيّن الشكل A.8 كيفيّة استجابة المستهلِكين بحسب ما أفادوا به

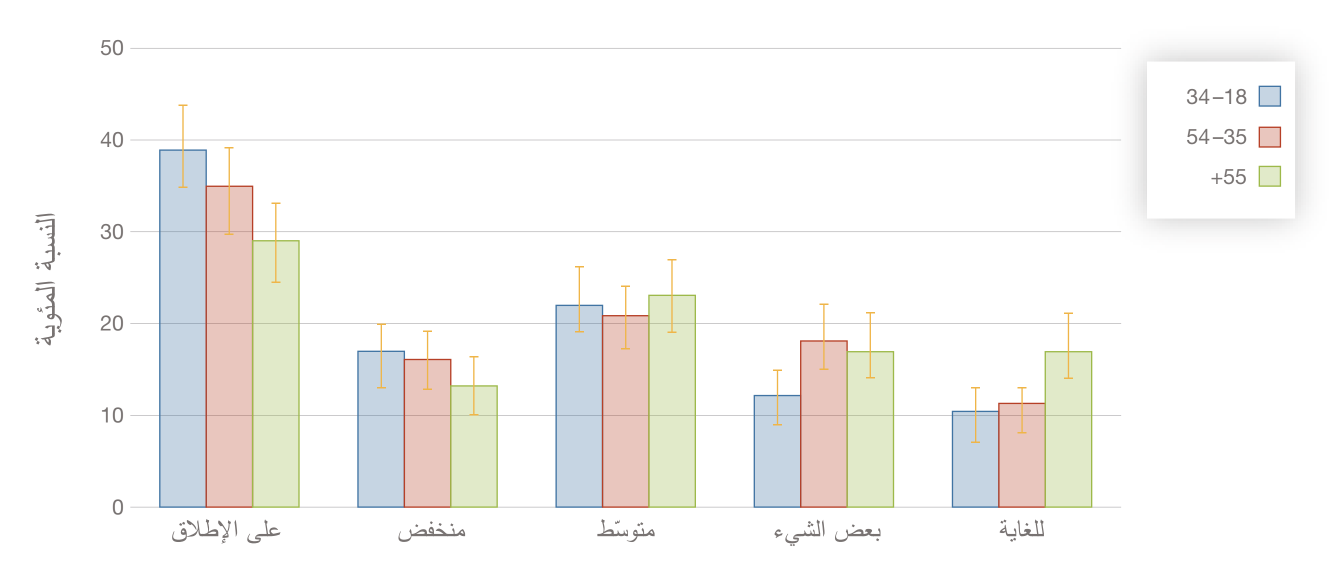
الشكل A.6

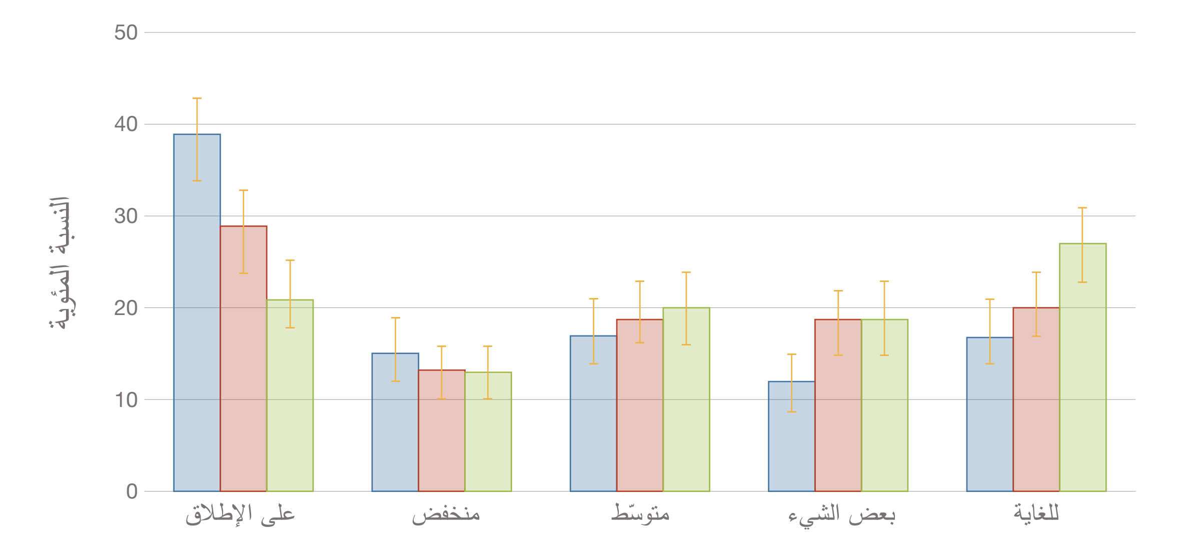
مستوى القلق بشأن عمليتَي اختراق تارجت (Target) وإكويفاكس (Equifax)



الشكل A.7

مستوى القلق، بحسب العمر، بشأن عمليتَي اختراق تارجت (Target) (في الأعلى) وإكويفاكس (Equifax) (في الأسفل)



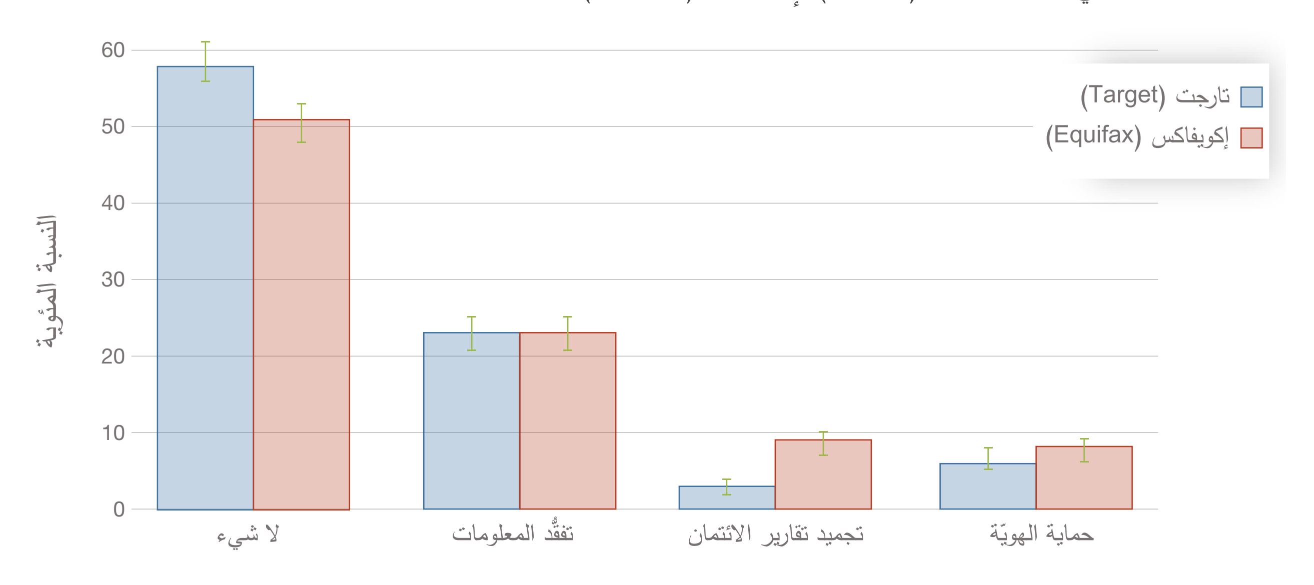


لعملية اختراق تارجت وعملية اختراق إكويفاكس. في حين أنّ الأغلبية لم تتّخِذ أي تدابير للاستجابة لأي من عمليتَي الاختراق، استجاب عدد أكبر بكثير من الأشخاص لعملية اختراق إكويفاكس عام 2017 مقارنةً بعملية اختراق تارجت عام 2013. وفي حين قامت نسبة متساوية من المجيبين بتفقّد أمن معلوماتها بعد كلّ عملية اختراق، جَمَّدَت نسبة مئوية أكبر بكثير من المجيبين جميع تقارير ائتمانها أو فقط تلك التي تملكها إكويفاكس بعد عملية اختراق إكويفاكس.

في حين لا تختلف الاستجابات المُفاد بها لعمليتَي اختراق تارجت وإكويفاكس بحسب الجنس، تبيّن النتائج أنّ الراشدين الأكبر سنّاً كانوا أكثر استجابةً على الأرجح من الراشدين الأصغر سناً. أمّا بالنسبة إلى عملية اختراق تارجت، فإنّ الفرْق الأساسي والمهمّ إحصائياً هو أنّ الراشدين الذين يبلغون 55 عاماً من العمر فأكبر كانوا أكثر أرجحيةً من الفئات العمرية الأصغر سناً للحدّ من التسوّق في تارجت أو للتوقُّف عنه تماماً بعد عملية الاختراق. فقد حدّ اثنا عشر في المئة من الفئة العمرية من 55 عاماً فأكبر من التسوّق في تارجت أو توقّفوا عنه، في حين حدّت نسبة 7 في المئة من الفئات العمرية الأصغر سنّاً من التسوّق في تارجت أو توقّفَت عنه. وبعد عملية اختراق إكويفاكس، جمّدت نسبة 5 في المئة من الفئة العمرية من 18 إلى 34 عاماً، ونسبة 9 في المئة من الفئة العمرية من 35 إلى 54 عاماً، ونسبة 12 في المئة من

الشكل A.8

الاستجابات لعمليتي اختراق تارجت (Target) وإكويفاكس (Equifax)



الفئة العمرية من 55 عاماً فأكبر تقارير الائتمان الخاصة بها. وبالمثل، اشترت نسبة 4 في المئة من الفئة العمرية من 18 إلى 34 عاماً، ونسبة 8 في المئة من الفئة العمرية من 35 إلى 54 عاماً، ونسبة 12 في المئة من الفئة العمرية من 55 عاماً فأكبر خدمة حماية الهوية وبدأت باستخدامها بعد عملية اختراق إكويفاكس.

التهديدات الافتراضية

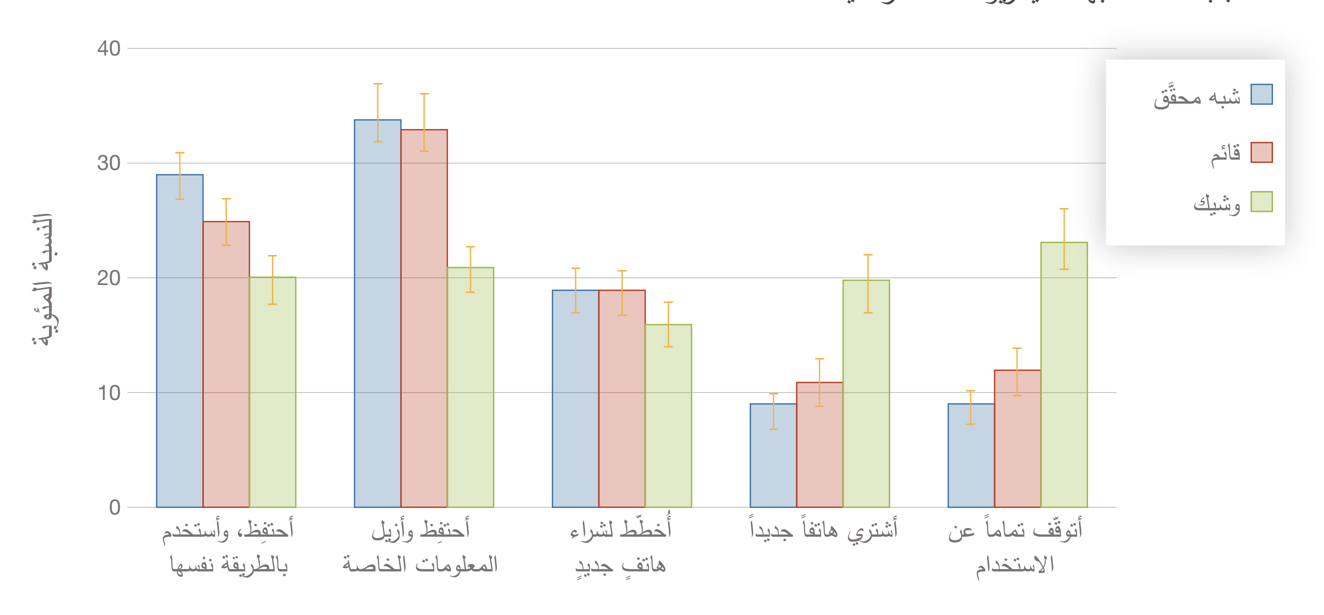
أخيراً، استخدمنا الدراسة الاستقصائية حول المستهلِكين لتقييم كيفية استجابة المستهلِكين للتهديدات المحتملة الناجمة عن حاسوبٍ كموميٍّ قادرٍ على اختراق التشفير باستخدام المفتاح العام الحالي. للقيام بذلك، عرضنا ثلاثة سيناريوهات افتراضية تتعلّق بتكنولوجيا قد تتيح للقراصنة التحكّم بهواتف المجيبين الذكية. يصِف السيناريو الأول التكنولوجيا على أنّها شبه متطوّرة ولكنّه يذكُر أنّ شركة تصنيع هاتف المجيب لم تقم بتثبيت أنظمة أمن جديدة لمنع عمليات الاختراق. في السيناريو الثاني، يمتلك القراصنة التكنولوجيا الجديدة، وقد تمّت قرصنة بعض الهواتف، ولم تُثبِّت بعد شركة تصنيع الهواتف الذكية أنظمة أمن جديدة. أخيراً، في السيناريو الثالث، تمّت قرصنة شركة تصنيع هواتف المجيبين الذكية وقد يستطيع القراصنة الآن رؤية كلّ ما يوجد على هواتف المجيبين الذكية والتحكم فيها. ولكلّ من هذه السيناريوهات، اختار المجيبون أحد الخيارات التالية: أحتفِظ بالهاتف وأستخدمه بالطريقة نفسها؛ أو أحتفِظ بالهاتف ولكنني أزيل عنه الأمور الخاصة؛ أو أُخطّط لشراء هاتفٍ جديدٍ وأكثر أمناً؛ أو أشتري هاتفاً جديداً وأكثر أمناً على الفور؛ أو أتوقف تماماً عن استخدام الهواتف الذكية.

تُعتبر النتائج الموضحة في الشكل A.9 متسقة منطقياً، فكلّما اقترب التهديد، زادت الاستجابة. وفي حين سيتّخذ جزء من المستهلِكين خطوات ملموسة بشكلٍ استباقيٍّ للحدّ من ضعفهم، لن يقوم المستهلِكون بشراء هاتفٍ ذكيٍّ جديدٍ أو لن يتوقّفوا عن استخدام هواتفهم الذكية إلّا عندما يكون التهديد الأكثر إلحاحاً. تكمن الاستجابة الأكثر شيوعاً للسيناريوهَين الأوّلَين في الاحتفاظ بنفس الهاتف الذكي ولكن مع إزالة المعلومات الخاصة منه. وتنطوي الاستجابة الثانية الأكثر شيوعاً للسيناريوهَين الأوّلَين على الاحتفاظ بنفس الهاتف الذكي واستخدامه بالطريقة نفسها. وقال حوالي 10 في المئة فقط من المجيبين إنّهم قد يشترون هاتفاً جديداً وأكثر أمناً في ظل السيناريوهَين الأوّلَين، وقال 10 في المئة من المجيبين الآخرين إنّهم قد يتوقّفون عن استخدام الهواتف الذكية بالكامل. في المقابل، أتَت الاستجابة الأكثر شيوعاً للسيناريو الثالث بالتوقّف عن استخدام الهواتف الذكية. بالمقارنة مع السيناريوهَين الأوّلَين، من المرجح بشكلٍ كبيرٍ أن يتوقف المجيبون عن استخدام الهواتف الذكية أو أن يشتروا هاتفاً ذكيّاً جديداً وأكثر أمناً استجابةً للسيناريو رقم 3. وبالمثل، إنّ أرجحيّة احتفاظ المجيبين بهواتفهم الذكية (إما لاستخدامها بنفس الطريقة، أو إزالة المعلومات الخاصة عنها، أو مع التخطيط لشراء هاتف جديد في المستقبل) استجابةً للسيناريو رقم 3، أدنى بكثير منه للسيناريوهين الآخرين.

هناك بعض أوجه الفرق المثيرة للاهتمام في الاستجابات بحسب العمر. بالنسبة إلى السيناريو الأول، من المرجح نسبيّاً أن تحتفظ الفئة العمرية التي تتراوح بين 18 و34 عاماً بهواتفها الذكية وتستخدمها بالطريقة نفسها (32 في

الشكل A.9

الاستجابات المُفاد بها للسيناريوهات الافتراضية



المئة مقارنةً بـ26 في المئة من الفئات العمرية الأكبر سنّاً). ومع ذلك، فإن الاستجابة الأكثر شيوعاً لدى الفئة العمرية التي تتراوح بين 18 و34 عاماً هي الاحتفاظ بالهاتف ولكن مع إزالة المعلومات الخاصة عنه (36 في المئة). إنّ هذه الاستجابة هي أيضاً الأكثر شيوعاً لدى الفئات العمرية الأكبر سنّاً. ففي هذا السيناريو، من الأكثر ترجيحاً أن يتوقّف المجيبون في الفئتين العمريتين من 35 إلى 54 عاماً ومن 55 عاماً فأكبر عن استخدام الهواتف الذكية مقارنةً بنظرائهم الأصغر سناً، ولكن قد لا تتّخِذ هذه الخطوة سوى نسبة 11 في المئة من الفئة العمرية من 55 عاماً فأكبر ونسبة 9 في المئة من الفئة العمرية بين 35 و54 عاماً. بالنسبة إلى المجيبين الذين تتراوح أعمارهم بين 18 و34 عاماً، فإن التغيير الرئيسي في السيناريو الثاني هو ازدياد أرجحية شراء هاتفٍ جديدٍ أو التوقّف عن استخدام أي هواتف ذكية، في حين تنخفض النسبة المئوية للذين يحتفظون بالهاتف ولكنّهم يزيلون المعلومات الخاصة عنه. ومن بين المجيبين في الفئتين العمريتين من 35 إلى 54 عاماً ومن 55 عاماً فأكبر، فإن التغيير الرئيسي هو انخفاض عدد المستخدِمين الذين يحتفظون بهواتفهم ويستخدمونها بالطريقة نفسها، بينما يحتفظ عددٌ أكبر من المجيبين بهواتفهم ويزيلون المعلومات الخاصة عنها. في السيناريو الثالث، تُظهر النتائج أنّ الاستجابة الأكثر شيوعاً لدى الفئة العمرية التي تتراوح بين 18 و34 عاماً هي عدم التصرّف، مع الاحتفاظ بهواتفهم الذكية واستخدامها بالطريقة نفسها (23 في المئة)، في حين ترتفع النسبة المئوية للذين قد يشترون هاتفاً ذكياً جديداً أكثر أمناً بحيث تكاد تلك النسبة المئوية تعادلها (22 في المئة). في المقابل، فإن الاستجابة الأكثر شيوعاً لهذا السيناريو بين الفئات العمرية الأكبر سنّاً هي التوقّف عن استخدام الهواتف الذكية (حوالي 27 في المئة).

بالنسبة إلى النساء، إنّ الاستجابة الأكثر شيوعاً لكلّ سيناريو هي الاحتفاظ بهواتفهن ولكن مع إزالة المعلومات الخاصة عنها. استجابةً للسيناريوهين رقم 1 ورقم 2، قد تحتفظ 40 في المئة من النساء بهواتفهن الذكية وتزيلن المعلومات الخاصة عنها، في حين أفادت نسبة 27 في المئة فقط من الرجال بالاستجابة نفسها. فاستجابةً للسيناريوهين رقم 1 ورقم 2، يُعتبر الرجال أكثر أرجحية للتخطيط لشراء هاتفٍ جديدٍ أو لشراء هاتف جديد فعليّاً أو للتوقّف تماماً عن استخدام هواتفهم الذكية. ومع ذلك، واستجابةً للسيناريو رقم 3، تزداد الأرجحية لإزالة المعلومات الخاصة عن الهواتف، أو للتخطيط لشراء هاتفٍ جديد، أو لشراء هاتفٍ جديدٍ فعليّاً لدى النساء. أمّا الرجال فهُم أكثر أرجحيةً للذهاب نحو الخيارات المتطرّفة: إمّا الاحتفاظ بهواتفهم الذكية واستخدامها بالطريقة نفسها، أو التوقّف تماماً عن استخدام الهواتف الذكية.

بالإضافة إلى التحليل الوصفي الآنف ذكره، استخدمنا أيضاً بيانات الدراسة الاستقصائية حول المستهلِكين لاستكشاف الارتباط بين الاستجابات النشطة للسيناريوهات الافتراضية وكيفية ردّ المستهلِكين على عمليتَي اختراق تارجت واكويفاكس. لذلك، حدّدنا أولاً أنّ استجابة نشطة تعني شراء هاتفٍ جديدٍ وأكثر أمناً على الفور أو التوقّف تماماً عن استخدام الهواتف الذكية. اعتبِر أنّ A_i يرمز إلى متغيرٍ

ثنائي يشير إلى استجابةٍ نشطة من قِبَل الفرد i. ثمّ اعتَبِر أنّ T_i يرمز إلى الاستجابة لعملية اختراق تارجت؛ وهو أيضاً مُتغيّر ثنائي، يساوي 0 في حال لم يقم الفرد i بأيّ استجابة و 1 إذا قام الفرد i بأيّ استجابة (تفقَّدَ أمن معلوماته، أو جمَّد تقارير الائتمان الخاصة به، أو بدأ باستخدام حماية الهوية، أو حدَّ من التسوق في تارجت/توقَّف عنه). بالإضافة إلى ذلك، اعتَبِر أنّ E_i متغيرٌ ثنائيٌّ يشير إلى أي استجابة لعملية اختراق إكويفاكس. أخيراً، اعتَبِر أنّ X_i يرمز إلى الخصائص الفردية. إننا نُدرج X_i لاستبعاد الاستجابات التفاضلية بحسب العمر والجنس وولاية الإقامة. نقدّر أنّ المعادلة التالية تظهر الارتباط بين الاستجابات لعمليتَي اختراق تارجت وإكويفاكس والاستجابة النشطة للسيناريوهات الافتراضية مع بقاء خصائص الفرد ثابتة:

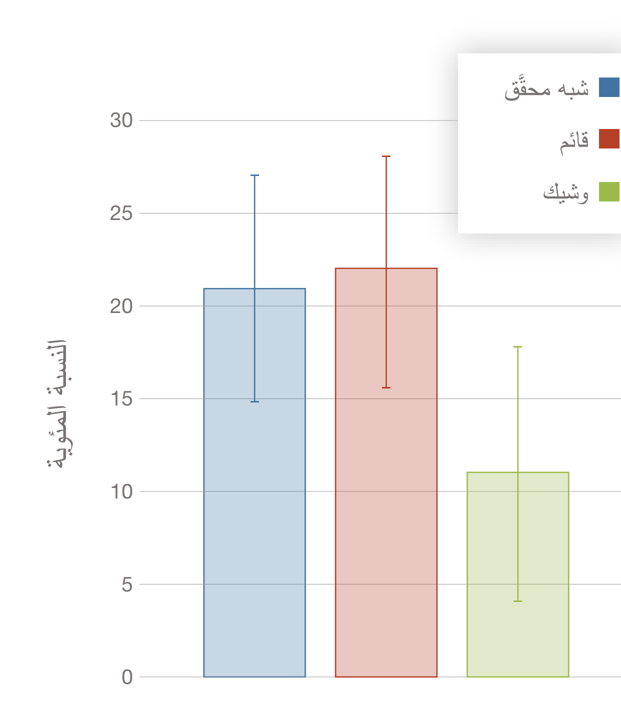
$$A_i = \alpha + \gamma T_i + \delta E_i + \theta X_i + \varepsilon_i \, .$$

إننا ندرس أولاً الارتباطات بين الاستجابات للسيناريوهات الافتراضية وعملية اختراق تارجت. إنّ الارتباطات التقديرية الموضّحة في الشكل A.10 هي نتيجة التقديرات وفق نموذج لوجت (الانحدار اللوجستي) (logit estimations) للمعادلة السابقة لكلّ من السيناريوهات الافتراضية الثلاثة. تشير هذه النتائج إلى ارتباطٍ إيجابيٍّ وهامٍ لأيّ استجابة لعملية اختراق تارجت مع استجابة نشطةٍ للسيناريوهين الافتراضيين الأوّلين (إمّا من خلال شراء هاتفٍ جديدٍ وأكثر أمناً على الفور أو التوقّف التام عن استخدام الهواتف الذكية). بالإضافة إلى ذلك، ترتبط أي استجابة لعملية اختراق تارجت بشكل إيجابي، ولكن بشكل غير هام، باستجابة نشطة للسيناريو الافتراضي الثالث. بشكلٍ عام، تشير هذه النتائج إلى أنّ الاستجابات لعملية اختراق تارجت هي مؤشرات على مستوى قلق المستهلِك بشأن الخصوصية. علاوةً على ذلك، تشير النتائج إلى أنّه من المحتمل أن تُحدّد الاستجابات لعملية اختراق تارجت جهات الانتقال الباكر، أو المستهلِكين الذين سيكونون من بين أولئك الذين يستجيبون أولاً لتهديدات الأمن الإلكتروني الناجمة عن تطوير حاسوبٍ كموميّ. من ناحية أخرى، يشير الارتباط الإيجابي ولكن غير الهام بين أي استجابة لعملية اختراق تارجت واستجابة نشطة للسيناريو الافتراضي الثالث إلى أنّه، بالنسبة إلى التهديدات الوشيكة الأوسع نطاقاً، سيستجيب عدد أكبر من الأشخاص بشكل نشِط وبالتالي تُعتبر التدابير المسبقة مؤشرات منبئة أقل إنارة.

بعد ذلك، ندرس في الشكل A.11 الارتباطات بين

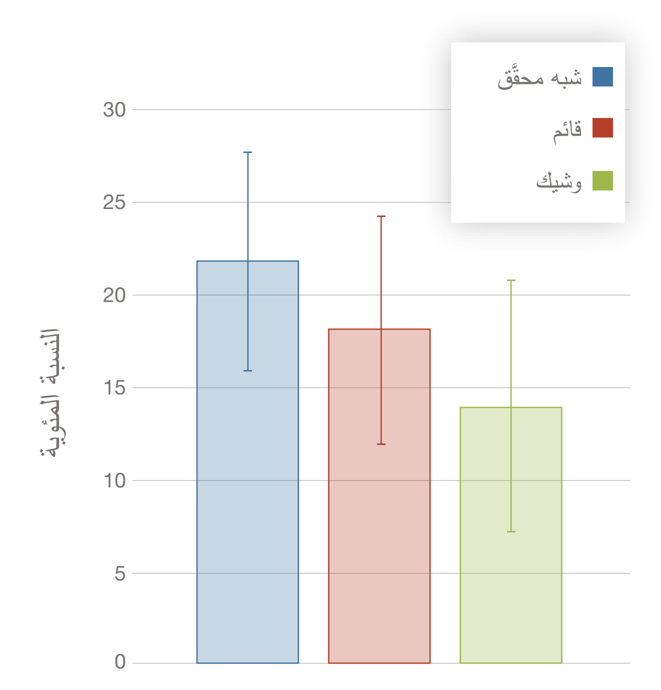
الشكل A.10

الارتباط التقديري بين الاستجابات النشطة للسيناريوهات الافتراضية وردود الفعل على عملية اختراق تارجت (Target)



الشكل A.11

الارتباط التقديري بين الاستجابات النشطة للسيناريوهات الافتراضية وردود الفعل على عملية اختراق إكويفاكس (Equifax)



الاستجابات للسيناريوهات الافتراضية وعملية اختراق إكويفاكس. تشير هذه النتائج إلى أنّ أي استجابة لعملية اختراق إكويفاكس ترتبط بشكلٍ إيجابيٍّ وهام باستجابة نشطة لجميع السيناريوهات الافتراضية (إمّا من خلال شراء هاتفٍ جديدٍ وأكثر أمناً على الفور أو التوقّف التام عن استخدام الهواتف الذكية). على نحو مشابه لنتائج تارجت، تشير هذه النتائج إلى أنّ الاستجابات لعملية اختراق إكويفاكس هي مؤشرات على مستوى قلق المستهلِك بشأن الخصوصية. ومثلما يُحتمل أن تُحدّد الاستجابات لعملية اختراق تارجت جهات الانتقال الباكر من بين المستهلِكين، كذلك الأمر بالنسبة إلى الاستجابات لعملية اختراق إكويفاكس التي تُحدّد المستهلِكين الذين سيكونون من بين أولئك الذين يستجيبون أولاً لتهديدات الأمن الإلكتروني الناجمة عن تطوير حاسوبٍ كموميّ.

الملحق B: المنهجية

إنّ تطوير حاسوبٍ كموميّ، والتهديد الذي يتعرّض له التشفير باستخدام المفتاح العام (PKC) الحالي والناجم عن حاسوبٍ كمومي، وتطوير حلول التشفير هي كلّها أحداث تنطوي على عدم يقين حول ما إذا كانت ستتحقّق ومتى ستحقّق. ومع ذلك، وبهدف تجنُّب الآثار الكارثية المحتملة لحاسوبٍ كموميٍّ ذي صلة بالتشفير في حوزة الجهات الفاعلة الخبيثة قبل أن يتمّ اعتماد حلول التشفير بشكلٍ ملائم، يتوجب على صانعي السياسات تصميم العلاجات الفعالة وتطبيقها في أقرب وقتٍ ممكن. لسوء الحظ، لا يمكن للبيانات الحالية وأدوات النمذجة أن تُزوِّد صانعي القرارات بجميع المعلومات المطلوبة لفهم الجدول الزمني للتهديد والمخاطر الأمنية المتوقَّعَة.

بسبب عدم ملاءمة البيانات والأدوات المتوفِّرَة، اخترنا استخدام مقاربة مختلطة الأساليب لإجراء هذا البحث. انطوت الخطوة الأولى على مراجعةٍ شاملةٍ للدراسات السابقة التي وفَّرَت فهماً أساسياً للأنماط التاريخية، والقضايا الحالية والتقدُّم المُستجِد في مجال تطوير الحوسبة الكمومية والأبحاث حول التشفير ما بعد الكمّ (PQC) وعمليات الانتقال إلى التشفير. فاستناداً إلى الرؤى المكتسَبة، طوّرنا استنباطاً لآراء الخبراء حول المخاطر الأمنية التي قد تنجم عن التطوير المستقبليّ لحاسوبٍ كموميٍّ قادر على اختراق التشفير باستخدام المفتاح العام الحالي، وطبّقناه. بالإضافة إلى ذلك، ساعَدَت مراجعة الدراسات السابقة في تحديد مجموعة أوّلية من الخبراء وشكَّلَت الأساس للأسئلة التي طرحناها. وتمثّلت الخطوة الأخيرة في مقاربتنا المختلطة الأساليب بإجراء دراسة استقصائية لعيّنة مرجّحة وتمثيلية من المستهلِكين على نطاق الوطن. تمّ تصميم الدراسة الاستقصائيّة لتقييم وعي المستهلِكين بالحوسبة الكمومية والتشفير، وكيفية استجابة المستهلِكين للحوادث الإلكترونية السابقة، وكيفية احتمالية استجابة المستهلِكين للتهديد الذي يشكله حاسوبٌ كمّوميٌّ قادر على اختراق التشفير باستخدام المفتاح العام الحالي. ويرِد فيما يلي وصْف المنهجيات المستخدَمة في هذه المقاربة المختلطة الأساليب وتفاصيل النتائج المُستخلَصة.

استنباط آراء الخبراء

يُعتبر استنباط آراء الخبراء إجراءً تم إضفاء الطابع الرسمي عليه وتوثيقه للحصول على أحكام الخبراء الاحتمالية وجمْعها (كولسن وكوك [Colson and Cooke]، 2018). في حين لا يُعتبر الأسلوب مناسباً لفحص الكميات التي يمكن ملاحظتها بشكلٍ تجريبيّ، تمّ استخدامه بنجاح لاستكشاف أسئلة ذات دعْمٍ تجريبي محدود وقابلة للقياس نظرياً ولكن ليس عملياً (كوك وغوسنز [Cooke and Goossens]، 2008). على سبيل المثال، غالباً ما أثبتَت دراسات الصحة البيئية الآثار السلبية للتعرّض للجُسيمات (particulate matter) (PM_{10} [جُسَيماتٌ يَقِلّ قُطْرُها عن 10 ميكرون] – التي يتراوح قُطْرُها بين 10 و2.5 ميكرومتر) والجُسَيمات الدقيقة (fine particulate matter) ($PM_{2.5}$ [جُسَيماتٌ يَقِلّ قُطْرُها عن 2.5 ميكرون] – التي يساوي قُطْرُها 2.5 ميكرومتر أو ما دون) باستخدام مقاييس يجري رصْدها لكلا النوعين من التلوث. في المقابل، لا يمكن التأكد من الآثار الصحية للجُسَيمات المتناهية الصغر ($PM_{0.1}$ – التي يساوي قُطْرُها 0.1 ميكرومتر أو ما دون) من خلال البحث التجريبي بسبب الافتقار إلى مقاييس الجُسَيمات المتناهية الصغر. وبسبب الافتقار إلى مقاييس تجريبيّة، استخدَم الباحثون استنباط آراء الخبراء لتقييم الأدلة حول وجود علاقة سببية بين الجُسَيمات المتناهية الصغر والصحة (نول وآخرون [Knol et al.]، 2009). يكون التغيّر المناخي المقارنة الأكثر ملاءمةً لمخاطر الحوسبة الكمومية الأمنية. كما هو الحال مع قوّة الحوسبة وسرعتها، يمكننا ملاحظة آثار التغيُّرات الخفيفة إلى المعتدلة في المناخ، ولكن يبقى الأساس التجريبي محدوداً للحكم على آثار تجاوُز العتبات الكبيرة في مجالي المناخ وقوّة الحوسبة وسرعتها. فقد تمّ استخدام استنباط آراء الخبراء لدراسة مختلف التأثيرات المحتملة لتغيُّر المناخ، بما في ذلك التأثيرات على الدوران التقلبي الجنوبي في المحيط الأطلسي (Atlantic Meridional Overturning Circulation) (زيكفيلد وآخرون [Zickfield et al.]، 2007) والأنظمة البيئية للغابات (مورغن، بيتلكا، وشيفلياكوفا [Morgan Pitelka and Shevliakova]، 2001).

تكمن أفضل الممارسات في أن توجِّه استنباطات آراء الخبراء جمْع البيانات، والنمذجة، والتحليل في المستقبل.

ولكن، لا يمكن دائماً الانتظار إلى أن تتوفَّر المقاييس التجريبية لتصميم السياسات. وبالتالي هذا هو الموضع المناسب حيث تُعتبر استنباطات آراء الخبراء الأنسب للاستخدام. ففي هذا السياق، تمّ استخدام استنباطات آراء الخبراء في مجموعة من المسائل تتراوح ما بين الأمان النووي وصولاً إلى النمو الاقتصادي (كولسون وكوك [Colson and Cooke، 2018). يمكن لاستنباط آراء الخبراء المُنَفَّذ بشكلٍ جيّدٍ أن يعوّض عن الفجوات المعرفية التي لا يمكن للبيانات والتحليل معالجتها وينير عملية تصميم السياسات مثل تلك التي تنطوي على مسألة تطوير الحوسبة الكمومية غير المؤكدة (كولسون وكوك [Colson and Cooke]، 2018). وتتطلّب استنباطات آراء الخبراء تصميماً دقيقاً واختباراً تجريبياً لبروتوكول المقابلات، واختيار الخبراء، وإجراء المقابلات ومن ثمّ التحليل (مورغن وهنريون [Morgan and Henrion]، 1990).

اختيار الخبراء

على عكس معظم الجهود الرامية إلى أخْذ العينات، لا تهدف استنباطات آراء الخبراء إلى الحصول على عينة تمثيلية إحصائياً بل إلى فهْم نطاق أحكام الخبراء المسؤولة (مورغن [Morgan]، 2014). وبالتالي، يجب اختيار الخبراء بعناية. عادةً، يجب اختيار الخبراء لتمثيل مجموعة متنوعة من المعرفة والخلفيات والآراء (كولسون وكوك [Colson and Cooke]، 2018). فقد استخدمنا مراجعة الدراسات السابقة لتحديد وجهات النظر والتفسيرات الرئيسية في المجالات ذات الصلة والتأكُّد من تمثيل كلّ منهما. بحثنا بشكلٍ أوليٍّ عن خبراء في ثلاثة مجالات: تطوير الحوسبة الكمومية، التشفير ما بعد الكم (PQC) وتطوير معايير التشفير، والأمن الإلكتروني للصناعة التجارية. فقد وفَّرت لنا مراجعة الدراسات السابقة أسماء عدد من الخبراء الذين نشروا مقالات في مجالات تطوير الحوسبة الكمومية، بالإضافة إلى التشفير ما بعد الكم وتطوير معايير التشفير. بالإضافة إلى الخبراء الذين تمّ تحديدهم خلال مراجعة الدراسات السابقة، وبهدف تشكيل قائمتنا الأولية للأشخاص الذين سنقابلهم، تواصلنا أيضاً في البداية مع أعضاء لجنة التقييم التقني لجدوى الحوسبة الكمومية وتأثيراتها التابعة للأكاديمية الوطنية للعلوم والهندسة والطبّ (National Academy of Sciences, Engineering, and Medicine Committee on the Technical Assessment of the Feasibility and Implications of Quantum Computing). بينما يتمّ اختيار الخبراء الأكاديميين بشكلٍ ملائمٍ بالاستناد إلى مراجعة الدراسات السابقة والتشاور مع الأكاديميات الوطنية، تُعَد الحوسبة الكمومية مجالاً لاستثمارات وأبحاث القطاع الخاص الكبيرة. في بعض الأحيان، يتمّ ذِكر خبراء من القطاع الخاص أو الإشارة إليهم في الدراسات السابقة، وقمنا بتضمين كلّ من هذه الأسماء التي وجدناها على اعتبار أنّه من المحتمل إجراء مقابلات معهم. بالإضافة إلى ذلك، وبهدف الوصول إلى بعض الشركات في القطاع الخاص ذات الأهمية، اعتمدنا على علاقات المؤلفين، التي أدّت بشكلٍ عام إلى إحالة موظف قد نستطيع إجراء مقابلة معه. أخيراً، حاولنا أيضاً الاتصال بعدد من الخبراء في القطاع الخاص من خلال استخدام أوصافهم المتوفِّرة على مواقع شركاتهم الإلكترونية.

أوصلتنا هذه الجهود إلى وضْع القائمة الأوّلية للأشخاص المحتملين لإجراء مقابلات معهم، ولكننا لم نختر كلّ الأشخاص المذكورين في هذه القائمة لإجراء مقابلة معهم. فبعد تحديد الأشخاص المحتملين لإجراء مقابلات معهم والاتصال بهم، اخترنا في النهاية خبراء بعد إجراء مراجعات لمؤهلاتهم و/أو محادثات أولية معهم حول المشروع ومدى ملاءمتهم للتحدّث عنه. انطبق هذا الأمر بشكلٍ خاص على خبراء القطاع الخاص لأنّ تقييم خلفياتهم وملاءمتهم كان أصعب من تقييم تلك الأمور بالنسبة للأكاديميين الذين لديهم منشورات متاحة للعامة.

وتمثّلت الخطوة الأخيرة التي اتخذناها لتحديد الخبراء واختيارهم بالمعاينة الجليدية (سلسلة الإحالة لأخذ العينات) (snowball sampling). في إطار استخدام هذا الأسلوب، طلبنا من الذين أُجريت معهم المقابلات تقديم توصيات أثناء إجراء المقابلات. عندما تمّ تحديد الأفراد من خلال المعاينة الجليدية، راجعنا أيضاً مؤهلاتهم و/أو أجرينا محادثات أولية لتقييم مدى ملاءمة خبرتهم لموضوع الدراسة. مرة أخرى، لم نختر كلّ الأشخاص الذين تمّت الإحالة إليهم لمقابلتهم.

في النهاية، تواصلنا مع 30 خبيراً أكاديمياً وصناعياً في مجال تطوير الحوسبة الكمومية، والتشفير ما بعد الكمّ وتطوير معايير التشفير، والأمن الإلكتروني للصناعة التجارية. ولأنّه لا توجد "إجابة صحيحة" عن السؤال "ما هو عدد الخبراء الذين نحتاج إليهم للحصول على استنباط جيّد للآراء؟" بدأنا باستهداف مجموعة مؤلفة من 12 إلى 21 خبيراً أردنا إجراء مقابلات معهم. سعينا إلى تنوّع خلفيات الخبراء من مجال الحوسبة الكمومية والتشفير، وأن يكونوا من المجال الأكاديمي والقطاع الخاص. وبعد التعرّف على الأشخاص المحتملين الملائمين لإجراء مقابلات معهم، تمّ تحديد عدد المقابلات النهائي من خلال عدد الإجابات بشكل عام، بالإضافة إلى عدد الإجابات من الخبراء الأكاديميين وخبراء القطاع الخاص. في نهاية المطاف، وافق 17 من هؤلاء الخبراء على أن تُجرى مقابلات معهم. لم يُجِب أربعة خبراء من الذين اتصلنا بهم بتاتاً، ورَفَض تسعة خبراء إجراء

مقابلات معهم لأسباب مختلفة، ومنها التضارُب في جدولة المقابلات. لقد أجرينا 15 مقابلة في المجموع لأنه من بين 17 خبيراً وافقوا على أن تُجرى مقابلات معهم، كانت هناك مجموعتان من شخصين من ذات المنظمة ورغبتا في إجراء المقابلة معاً. ويكمن الأمر المهم في أنّ الخبراء وافقوا على أن تُجرى مقابلتهم إما من دون نسْب المقابلة لهم أو من دون الكشف عن هويتهم، وتمكنّوا بالتالي من رفْض الإجابة عن أي سؤال. لقد أخطأنا بعدم نسْب المقابلات إلى الخبراء في مقابل عدم الكشف عن هويتهم، في محاولة للوفاء بتوصيات م. ج. مورغن (M.G. Morgan) (2014)، وبالتحديد لأنّ "الإفراط في عدم الكشف عن الهوية قد يؤدي إلى أخْذ تلك الأحكام بقدر أقل من الجدية." ومع ذلك، نظراً لأنّنا كنّا نجري مقابلات مع خبراء من القطاع الخاص حول مواضيع حساسة، عرضنا عليهم أيضاً عدم الكشف عن هويتهم إذا فضّلوا ذلك. كما رفَض أيضاً الخبراء أحياناً الإجابة عن الأسئلة وذلك لأسباب متعدّدة تتراوح من عدم وجود رأي حول الموضوع إلى وجود معلومات حساسة.

يحتوي المربّع النصّي في هذه الصفحة على أسماء الأشخاص الذين أُجريت معهم المقابلات ومناصبهم (عندما وافق الخبراء على ذلك) أو على مناصبهم فحسب (عندما طلبوا عدم الكشف عن هويتهم).

تصميم بروتوكول المقابلة

تناقش مراجعات الممارسات الفضلى في استنباط آراء الخبراء الحاجة إلى صياغة الأسئلة وهيكلة التدفّق العام لعملية الاستنباط بعناية لتحديد معتقدات الخبراء المذكورة على شكل احتمالات تحديداً دقيقاً (كولسون وكوك [Colson and Cooke]، 2018). لقد اتّبَع البروتوكول الذي صممناه مَثَّل كورترايت، مورغن، وكيث (Curtright, Morgan and Keith) (2008) كما هو مشار إليه في مورغن (Morgan) (2014).

تمّ تطوير البروتوكول من خلال التكرارات المتعدّدة، والتشاور مع ممارسين لاستنباط آراء الخبراء، والإرشاد. فقد هَدَفَ البروتوكول إلى استنباط استجابات هيكليّة بشأن الجدول الزمني لتطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير، والجدول الزمني لتوحيد معايير التشفير ما بعد الكمّ (PQC) واعتماده، وحجم المخاطر الأمنية في ظل سيناريوهات مستقبلية افتراضية. بالإضافة إلى ذلك، أردنا تضمين مكونات أقل هيكليّةً للمقابلات التي قد يُناقِش خلالها الخبراء أيّ قضايا تتعلّق بمخاطر الحوسبة الكمومية الأمنية التي يفكّرون بها، بالإضافة إلى القضايا، أو العوامل، أو العواقب التي لم نناقشها ضمن مكوِّن البروتوكول الهيكلي. بعد تكرارات متعدّدة للبروتوكول بين المؤلفَين، تشاورنا مع ممارسين آخرين

قائمة الأشخاص الذين أُجريت معهم المقابلات

داستن مودي (Dustin Moody)
عالِم رياضيات، مجموعة تكنولوجيا التشفير (Cryptographic Technology Group)، المعهد الوطني للمعايير والتكنولوجيا (NIST)

جون مارتينيز (John Martinis)
مدير قسْم المعدات الحاسوبية الكمومية، جوجل (Quantum Hardware Lead, Google)

كرايج موندي (Craig Mundie)
مالك شركة موندي وشركاه ش.م.م. (Mundie & Associates, LLC)

ليلي تشين (Lily Chen)
قائدة مشروع، مجموعة تكنولوجيا التشفير (Cryptographic Technology Group)، المعهد الوطني للمعايير والتكنولوجيا (NIST)

ميشيل موسكا (Michele Mosca)
أستاذ، جامعة واترلو (University of Waterloo)

سوزان كوبرسميث (Susan Coppersmith)
أستاذة، جامعة ويسكونسن–ماديسون (University of Wisconsin–Madison)

روبرت بلاكلي (Robert Blakley)
الرئيس العالمي لابتكار أمن المعلومات (Information Security Innovation)، سيتي غروب (Citigroup)

براين لاماكيا (Brian LaMacchia)
مدير قسْم الأمن والتشفير، قسْم الأبحاث التابع لمايكروسوفت (Microsoft Research)

بروس شناير (Bruce Schneier)
مدير قسْم التكنولوجيا، شركة آي بي إم ريزيلينت (IBM Resilient)

مارك جاكسون (Marc Jackson)
مدير قسْم العلوم، حوسبة كامبريدج الكمومية (Cambridge Quantum Computing)

توبي جويس (Toby Joyce)
حوسبة كامبريدج الكمومية (Cambridge Quantum Computing)

تشارلز طحان (Charles Tahan)
فيزيائي، مختبر العلوم الفيزيائية (Laboratory for Physical Sciences)

مدير الأبحاث
شركة تكنولوجيا الحوسبة (Computing Technology Company)

مشفِّر
شركة تكنولوجيا الحوسبة (Computing Technology Company)

مدير أمن المعلومات
قطاع الخدمات المالية

مدير أمن المعلومات
قطاع الاتصالات

مهندس الأمن الإلكتروني
شركة معدات حاسوبية للشبكات

لاستنباط آراء الخبراء. وأخيراً، قمنا بإرشاد البروتوكول لتقييم الصياغة والوضوح والتوقيت.

احتوى البروتوكول الذي طوّرناه على ستة أقسام. أولاً، وضعنا مقدمة إلى أهداف المشروع. ثانياً، وفّرنا معلومات أساسية عن التهديدات المحتملة التي قد تعترض الأمن الإلكتروني والناجمة عن الحواسيب الكمومية. لدى طرحنا الأسئلة على الخبراء، برزَت عناصر من بحثنا لم يكن جميع الخبراء مطلعين عليها. فكان الخبراء المتخصّصون في القضايا الهندسية للحواسيب الكمومية أقل اطلاعاً على التداعيات الأمنية، وكان خبراء الأمن أقل اطلاعاً على الجدول الزمني لتطوير الحوسبة الكمومية، وهلُم جرّاً. جرى في القسْم الثالث من البروتوكول طرْح سؤالٍ مفتوحٍ حول توقّعات الخبراء بشأن المخاطر الأمنية الناجمة عن حاسوبٍ كموميٍّ ذي صلة بالتشفير. فقد سعينا من خلال هذا السؤال إلى فهْم بعض القضايا الرئيسية التي كانت تشغل الخبراء، بالإضافة إلى تعزيز المناقشة التي قد تساعد في فهْم الاستدلال المؤدي إلى التقديرات الكميّة التي استنبطناها في الأقسام اللاحقة فهماً أفضل. وفي القسْم الرابع، طرحنا ثلاثة سيناريوهات افتراضية وطلبنا من الخبراء تقييم حجم العواقب. لقد وصَف السيناريو الأول الذي عرضناه مستقبلاً يتمّ فيه ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير قبل توحيد معايير التشفير ما بعد الكمّ. ووَصَف السيناريو الثاني الذي طرحناه مستقبلاً يتمّ فيه ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير بعد وقت قصير من توحيد معايير التشفير ما بعد الكمّ، فور البدء بالاعتماد. أمّا السيناريو الثالث الذي عرضناه فوصَف مستقبلاً يتمّ فيه ابتكار حاسوبٍ كموميٍّ ذي صلة بالتشفير بعد عشرة أعوام من توحيد معايير التشفير ما بعد الكمّ. ولكلّ من هذه السيناريوهات، طلبنا من الخبراء أن يقيّموا بشكلٍ منفصلٍ العواقب المترتبة على مؤسسة الدفاع والاستخبارات الأمريكية (U.S. defense and intelligence establishment)، والوكالات الحكومية الأمريكية الأخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، وصناعات التكنولوجيا الأقلّ تقدُّماً في القطاع الخاص. في القسْم الخامس، سألنا الخبراء عن الجداول الزمنية المرجّحة لابتكار الحوسبة الكمومية والتشفير ما بعد الكمّ وبعض التكنولوجيات المرتبطة بها ومدة اعتمادها. لقد استنبطنا جداول زمنية لظهور حاسوب كمومي ذي صلة بالتشفير، أو حاسوبٍ كموميٍّ قادر على اختراق التشفير باستخدام المفتاح العام الحالي. بالإضافة إلى ذلك، سألنا عن الجداول الزمنية لاعتماد الحكومة الأمريكية حاسوباً كمومياً ذا صلة بالتشفير، واعتماد جهة فاعلة حكومية خبيثة لحاسوبٍ كمّوميٍّ ذي صلة بالتشفير، واعتماد جهة فاعلة غير حكومية خبيثة لحاسوبٍ كمّوميٍّ ذي صلة بالتشفير. أخيراً، استنبطنا جداول زمنية لابتكار مجموعة خوارزميات أمان آمنة في وجْه هجوم كموميٍّ واعتمادها من قِبَل مؤسسة الدفاع والاستخبارات الأمريكية، ووكالات حكومية أمريكية أخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، وصناعات التكنولوجيا الأقلّ تقدُّماً في القطاع الخاص. في القسْم الأخير من البروتوكول، نختتم بأسئلة مفتوحة مختلفة لمناقشة القضايا التي لم يتمّ تناولها في البروتوكول، والمجالات الأخرى ذات الأهميّة التي حدّدناها خلال مراجعة الدراسات السابقة، وأي أفكار متعلّقة بأسئلة بحثنا رَغِبَ الخبراء في الإعراب عنها. إنّ البروتوكول الكامل متوفّر في الملحق C.

ومن بين القضايا الرئيسية التي تناولناها في تطوير البروتوكول كانت وسائل الاستدلال المعرفي، وعدم اليقين، والنطاق. نظراً لأن الأشخاص يميلون إلى الاستدلال المعرفي "الترسيخ والتعديل" أو ترسيخ قيمة أوليّة ومن ثم تعديلها صعوداً أو نزولاً، قلّصنا من تأثير هذا الاستدلال من خلال استنباط القِيَم القصوى قبل الإدلاء بأفضل تقدير (تفيرسكي وكانيمان [Tversky and Kahnemean]، 1974؛ مورغن [Morgan]، 2014). إنّ هذه القضية ذات صلة خاصة بالجداول الزمنية لتطوير الحوسبة الكمومية وتوحيد معايير التشفير ما بعد الكمّ واعتماده. في هذه الحالات، طلبنا من الخبراء أولاً "الإفادة بأقرب عام ممكن قد يتمّ فيه تطوير التكنولوجيا أو قد يقع الحدث خلاله." ثم سألنا عن "أبعد عامٍ ممكن" يليه "أفضل تقدير لعام حدوث هذا الأمر." ترتبط قضية عدم اليقين بترتيب الأسئلة. فنظراً لصعوبة التفكير احتماليّاً، لا سيما بشأن الأحداث النادرة أو المستقبلية، تخضع التقديرات بشكلٍ عام للثقة المفرطة، ممّا يحدّ من عدم اليقين. ولمعالجة هذا الأمر، تابعنا استنباطات حول القِيَمَ القصوى من خلال أسئلة حول أي أمور قد تُغيِّر هذه القِيَم (مورغن [Morgan]، 2014). بشكلٍ محدّد، بعد طرْح السؤال عن "أقرب عامٍ ممكن" و"أبعد عام ممكن" فيما يتعلّق بالأسئلة المرتبطة بالجدول الزمني، طلبنا من الخبراء "تخيُّل أيّ ظرف ممكن قد يقع فيه الحدث في وقتٍ سابقٍ [لاحق]. إذا استَطَعْتَ التفكير في مثل هذه الظروف، يرجى مراجعة تقديراتك وفقاً لذلك." أخيراً، نظراً لعدم اليقين فيما يتعلّق بنطاق التهديدات الحالية على الأمن الإلكتروني، من الصعب التأكُّد من نطاق مناسب لوصف حجم التهديدات المستقبلية على الأمن الإلكتروني التي قد تُسبّبها الحوسبة الكمومية. تشكِّل قضية النطاق إشكالية لدى تقييمنا لحجم المخاطر الأمنية في ظل السيناريوهات المستقبلية الافتراضية. لمعالجة هذه المسألة، سعينا إلى إنشاء نطاقات بسيطة تتضمّن العواقب الأكثر مباشرةً للتهديدات المحتملة. بالتحديد، طلبنا من الخبراء ترتيب عواقب السيناريوهات الافتراضية على نطاقات من 1 إلى 3، حيث يصِف الرقم 1 الوصول أحياناً إلى المعلومات الحساسة، ويصِف الرقم 2 الوصول في كثير

من الأحيان إلى المعلومات الحساسة، بينما يصف الرقم 3 السيطرة الكاملة على أنظمة المعلومات.

لقد حدّد مؤلّفا هذا التقرير الخبراء واتّصلا بهم واختاراهم. بعد موافقة مجلس المراجعة المؤسساتية، جدوَل المؤلفان المقابلات وأجرياها خلال فترة ثلاثة أشهُر تقريباً بين 11 مايو/أيار 2018 و16 أغسطس/آب 2018. وقبل إجراء المقابلات، تم إرسال بروتوكول المقابلة إلى الخبراء، بالإضافة إلى استمارة موافقة، واستمارة للإفادة ذاتياً على نطاقات من 1 إلى 5 بخبرتهم في مجالات تطوير الحوسبة الكمومية واعتمادها وتطوير التشفير ما بعد الكمّ واعتماده. في بداية كلّ مقابلة، تحقَّقَ المؤلفان ممّا إذا تمّ ملء استمارة الموافقة؛ في حال عدم ملئها، قرآها بصوت عالٍ وحصلا على الموافقة قبل بدء المقابلة. وشملت استمارة الموافقة فقرة للموافقة على إجراء تسجيل صوتي. في حال موافقة الخبراء على التسجيل الصوتي، بدأ المؤلفان بالتسجيل ومن ثم شرعا في المقابلة. وبعد إجراء المقابلات، تمّ تدوين التسجيلات.

خطّة تحليل الاستنباط

كانت خطتنا العامة لتحليل البيانات التي استنبطناها من الخبراء الذين اخترناهم وقابلناهم وصفيّة. لقد وصفنا الجداول الزمنية المستنبطة لتطوير حاسوبٍ كموميٍّ ذي صلة بالتشفير والجداول الزمنية المستنبطة لتوحيد معايير التشفير ما بعد الكمّ (PQC) واعتماده، ووصفنا أحجام المخاطر الأمنية المستنبطة في ظل سيناريوهات مستقبلية افتراضية. وقارنّا هذه التقديرات المستنبطة من الخبراء الذين تمّ جمْعهم بحسب خلفيتهم: خبير عام أو أكاديمي، وخبير في القطاع.

إضافةً إلى وصْف التقديرات المستنبطة من كلّ خبير، قمنا بإنتاج تقديرات مجمّعة. يجب تفسير المعامِلات المجمّعة التي تجمع أحكام العينات الصغيرة وغير التمثيلية بحذر. ثمّة أساليب مختلفة للوصول إلى الأساليب المجمّعة. لم يشمل استنباطنا لآراء الخبراء أساليب سلوكية للجمع ما بين آراء الخبراء، مثل أسلوب دلفي (Delphi method) (رو ورايت [Rowe and Wright]، 1999). بدلاً من ذلك، استخدمنا أساليب رياضية للجمع ما بين آراء الخبراء. يتضمّن الأسلوب الكلاسيكي للجمع ما بين آراء الخبراء رياضياً أيضاً طرْح أسئلة معايرةٍ حول القِيَم غير المؤكدة بالنسبة إلى الخبراء ولكن المعروفة من المحلّلين (كليمن ووينكلر [Clemen and Winkler]، 2007). بسبب طبيعة الحوسبة الكمومية وأبحاث التشفير ما بعد الكمّ السريعة التطوّر، وعدم اليقين المحيط بكلّ منهما، والأبحاث والتقدّمات المحصورة الملكية و/أو السرية المحرزة، ارتأينا أنّ أسئلة المعايرة قد لا تكون مجدية. عوضاً عن ذلك، طلبنا من الخبراء تقديم تقييمٍ ذاتي لخبرتهم في مجال تطوير الحوسبة الكمومية واعتمادها، بالإضافة إلى تطوير التشفير ما بعد الكمّ واعتماده. علاوةً على ذلك، طلبنا من الخبراء تقديم تقييمٍ ذاتي لخبرتهم في مختلف القطاعات التي نتطرّق إليها: مؤسسة الدفاع والاستخبارات الأمريكية (U.S. defense and intelligence establishment)، والوكالات الحكومية الأمريكية الأخرى، وصناعات التكنولوجيا المتقدّمة في القطاع الخاص، وصناعات التكنولوجيا الأقلّ تقدُّماً في القطاع الخاص. أُعطِيَت التقييمات على نطاقات من 1 إلى 5. بالإضافة إلى ذلك، قدّم المؤلّفان اللذان أجريا المقابلات تقييمات مستقلة لخبرة كلّ خبير على نطاقات من 1 إلى 5. كانت خمسة وثمانون في المئة من تقييمات الخبراء الذاتية وتقييمات الأشخاص الذين قابلناهم المستقلة متساوية أو على بُعد نقطة واحدة البعض منها من البعض الآخر على هذا النطاق. على إثر تقييمات المؤلِّفَين المستقلة، تمّ حلّ الخلافات من خلال مراجعة تكرارية إلى أن تمّ التوصّل إلى إجماع.

لقد مكّنتنا تقييمات الخبرة من إنتاج تقديرات مجمّعة بحسب المتوسط المرجّح بالاستناد إلى الخبرة. وبالتالي، بالإضافة إلى عرْض التقديرات المستنبطة من كلّ خبير، أظهرنا المتوسطات المرجحّة بالاستناد إلى الخبرة للجداول الزمنية لتطوير الحوسبة الكمومية والتشفير ما بعد الكمّ وأحجام المخاطر الأمنية الناجمة عن السيناريوهات الافتراضية. بالإضافة إلى ذلك، تمّ تفصيل كلّ منها بحسب خلفية الخبراء: خبير عام أو أكاديمي، وخبير في القطاع.

الدراسة الاستقصائية حول المستهلِكين

بعد مراجعة الدراسات السابقة واستنباط آراء الخبراء، صمّمنا دراسة استقصائيّة لاستكشاف الوعي بالحوسبة الكمومية والتشفير، والاستجابات للحوادث الإلكترونية السابقة، والاستجابات المحتملة للتهديد الناجم عن حاسوبٍ كموميٍّ قادر على اختراق التشفير باستخدام المفتاح العام الحالي. تتخطّى هذه الأسئلة نطاق اختصاص الخبراء الذين قابلناهم. بطبيعة الحال، لن يُمثّل وعي الخبراء واستجاباتهم للمخاطر المعقّدة الناجمة عن حاسوبٍ كموميٍّ ذي صلة بالتشفير المجموعة الأوسع. نتيجةً لذلك، قُمنا باستكشاف هذه الأسئلة بالاستناد إلى عينة من المستهلِكين الرقميين النشطين الذين هم أكثر عُرضة للآثار السلبية المستقبلية المحتملة الناجمة عن حاسوبٍ كموميٍّ ذي صلة بالتشفير. يصف مصطلح المستهلِكين الرقميين النشطين الغالبية الشاسعة من الأمريكيين في عام 2018. ففي عام 2018، بَلَغَت نسبة الراشدين الأمريكيين الذين يستخدِمون الإنترنت 89 في المئة، مع معدلات استخدام عالية على امتداد جميع المجموعات الديموغرافية (سميث وأندرسن [Smith and Anderson]، 2018).

تُضاف هذه الدراسة الاستقصائية حول المستهلِكين والتحليل اللاحق إلى العدد الصغير من الدراسات التي تطرّقت إلى منظور المستهلِكين حول عمليات اختراق الأمن الإلكتروني على مثال دراسة أبلون وآخرين (Ablon et al.) (2016). في حين أنّ الدراسات السابقة قد نظَرَت في مواقف المستهلِكين إزاء عمليات اختراق البيانات والاستجابات اللاحقة من قِبَل الشركات، هدفْنا إلى فهْم مجموعة التدابير التي قد يتخذها المستهلِكون ردّاً على مستويات عمليات الاختراق المختلفة، وفهْم كيف قد تُترجم تلك التدابير إلى المخاطر الفريدة التي تشكِّلها الحوسبة الكمومية على التشفير باستخدام المفتاح العام.

تمتدّ تداعيات أسئلتنا حول الوعي والاستجابات للخطر من المنظمات الفردية إلى الاقتصاد العالمي الحديث. من ناحية، إذا كان المستهلِكون قلقين بشأن أمن معلوماتهم الشخصية والمالية وغيرها من المعلومات الخاصة التي تنطوي عليها التفاعلات الرقمية، قد يقلّلون من تواجدهم على الإنترنت أو يوقفونه. ونظراً إلى الانتقال من التفاعلات التناظرية إلى الرقمية في عددٍ كبيرٍ من الخدمات، بدءاً من الخدمات الاجتماعية إلى الخدمات المصرفية ووصولاً إلى الرعاية الصحية، قد تشكِّل هذه الإمكانية ضربةً كبيرة لمنظمات محدّدة لا تتخذ الخطوات الاحترازية اللازمة وللاقتصاد العالمي الحديث ككلّ. من ناحية أخرى، قد تشير الأدلة من تدهور الأمن الإلكتروني الحديث إلى أنّ المستهلِكين إما يولون قيمة أقلّ لخصوصية معلوماتهم بالمقارنة مع الخدمات التي يتلقونها في المقابل، أو أنّهم يشعرون بأنّهم لا يملكون القوة على التحكُّم في خصوصية معلوماتهم. في هذه الحالة، يمكن التخفيف من الآثار السلبية الرئيسية على الاقتصاد العالمي.

تصميم دراسات جوجل الاستقصائية حول المستهلِكين (Google Consumer Survey)

لقد استخدمنا دراسات جوجل الاستقصائية حول المستهلِكين (Google Consumer Surveys [GCS]) لجمع عينة مرجّحة وتمثيليّة وطنياً من المستهلِكين لاستكشاف الوعي بالحوسبة الكمومية والتشفير، والاستجابات للحوادث الإلكترونية السابقة، والاستجابات المحتملة للتهديد الذي يشكله حاسوب كموميّ قادر على اختراق التشفير باستخدام المفتاح العام الحالي. فقد أجرينا دراسةً استقصائية شَمَلَت 1,100 مجيب تحتوي على عشرة أسئلة مصمَّمة انطلاقاً من المعرفة التي اكتسبناها من خلال مراجعة الدراسات السابقة واستنباط آراء الخبراء.

تُعتبر دراسات جوجل الاستقصائية حول المستهلِكين دراسات استقصائية على الإنترنت وقائمة على الاحتمالات وهي جديدة في سوق الدراسات الاستقصائية على الإنترنت المتنامية. فقد تطوّرت أبحاث الدراسات الاستقصائية من كونها مقابلات تُجرى وجهاً لوجه، إلى دراسات استقصائية هاتفية ابتداءاً من السبعينيات، لتصبح في الأعوام العشرة الماضية دراسات استقصائية على الإنترنت (ماكدونالد، محبي، وسلاتكين [McDonald, Mohebbi and Slatkin]، 2012). تنتج الدراسات الاستقصائية عينة تمثيلية قائمة على الاحتمالات باستخدام الخصائص الديموغرافية المستدلة من المعلومات حول أنواع المواقع الإلكترونية التي زارها المجيبون. يتمّ تحديد المجموعات المستهدَفة من الراشدين في الولايات المتحدة من أحدَث المسوحات للسكان الحاليين (Current Population Survey) وتتشكّل من التوزيع المشترَك للفئة العمرية والجنس والموقع (ماكدونالد، محبي، وسلاتكين [McDonald, Mohebbi and Slatkin]، 2012). تستخدِم دراسات جوجل الاستقصائية حول المستهلِكين أيضاً ترجيحاً ما بعد الطباقية (post–stratification weighting) للتعويض عن أوجه القصور في العينة والحدّ من انحياز العينة (ماكدونالد، محبي، وسلاتكين [McDonald, Mohebbi, and Slatkin]، 2012). في سياق مقارنة بين الديموغرافيات المستدلة والديموغرافيات المفاد بها، أظهَر مركز بيو للأبحاث (Pew Research) أنّه على الرغم من وجود أخطاء على مستوى المجيبين الأفراد، تتّسق الارتباطات ما بين الأسئلة الجوهرية والديموغرافيات مع تلك المبيَّنة في الدراسات الاستقصائية والديموغرافيات المفاد بها (كيتر وكريستيان [Keeter and Christian]، 2012). وقارن تشانج وكروسنيك (Chang and Krosnick) (2009) الاتصال العشوائي بالأرقام (random digit dialing) بدراسة استقصائية على الإنترنت قائمة على الاحتمالات وبدراسة استقصائية على الإنترنت غير قائمة على الاحتمالات خلال الانتخابات الرئاسية لعام 2000. تشير النتائج إلى أنّ الدراسات الاستقصائية على الإنترنت القائمة على الاحتمالات يمكن أن تُعطي نتائج أكثر دقّةً من الاتصال العشوائي بالأرقام والدراسات الاستقصائية غير القائمة على الاحتمالات (ماكدونالد، محبي، وسلاتكين [McDonald, Mohebbi and Slatkin]، 2012). تُعتَبَر تمثيليّة دراسات جوجل الاستقصائية حول المستهلِكين أساسيّةً لنتائجنا، ولكن، حتى إذا كانت دراسات جوجل الاستقصائية حول المستهلِكين الأكثر تمثيلاً لمجموعة السكان التي تستخدِم الإنترنت، تبقى ملائمة لدراستنا.

بالإضافة إلى ذلك، تم تصميم دراسات جوجل الاستقصائية حول المستهلِكين لتكون رخيصة، وتتصف بعبء استجابة منخفض، وتوفّر السرعة من حيث الفترات الزمنيّة الكاملة المطلوبة لتأدية المهمّة. تصل تكلفة دراسات

جوجل الاستقصائية حول المستهلِكين إلى 0.10 دولار أمريكي لكلّ إجابة عن كلّ سؤال. تقتصر دراسات جوجل الاستقصائية حول المستهلِكين على عشرة أسئلة، والتي، إلى جانب عبء النقر المنخفض، تؤدي إلى معدّل إجابة متوسط يساوي 16.75 في المئة مقارنةً بأقل من 1 في المئة لمعظم الدراسات الاستقصائية على الإنترنت (لافراكاس [Lavrakas]، 2010)، 7 في المئة إلى 14 في المئة للدراسات الاستقصائية الهاتفية (مركز بيو للأبحاث [Pew Research Center]، 2011). تقدّم دراسات جوجل الاستقصائية حول المستهلِكين أيضاً فوائد سرعة الفترات الزمنيّة الكاملة المطلوبة لتأدية المهمّة: يتم استكمال الدراسات الاستقصائية عادةً في غضون أسبوع واحد (سانتوزو، وشتاين، وستيفنسون [Santoso, Stein and Stevenson]، 2016).

لقد صمّمنا دراستنا الاستقصائية من خلال تكرارات متعدّدة واختبارات إرشادية متعدّدة. بعد إجراء تكرارات متعدّدة للدراسة الاستقصائية بين المؤلفَين، قمنا بإرشاد الدراسة الاستقصائية لتقييم الصياغة والوضوح والتوقيت. أجرينا اختبارات إرشادية مع زملاء من الخبراء في منهجيات الدراسات الاستقصائية بالإضافة إلى عدد من المجيبين المحتملين من غير الخبراء. يمكن الاطلاع على الدراسة الاستقصائية الكاملة على الإنترنت في الملحق C.

احتوت الدراسة الاستقصائيّة التي صمّمناها على عشرة أسئلة مقسّمة إلى ثلاثة أقسام مصمَّمة لمعالجة ثلاثة أهداف مختلفة. في القسْم الأول، كان الهدف فهْم مستوى الوعي. طرحنا أسئلة لتقييم الوعي بالحوسبة الكمومية والتشفير والآثار المحتملة على الأمن الإلكتروني الناجمة عن الحوسبة الكمومية. في القسْم الثاني، كان الهدف تقييم كيفية استجابة المستهلِكين وشعورهم تجاه عمليات اختراق الأمن الإلكتروني السابقة. وقد ناقشنا بإيجاز عمليتَي الاختراق الحديثتين لتارجت (Target) (والاس [Wallace]، 2013) وإكويفاكس (Equifax) (برنارد وآخرون [Bernard et al.]، 2017). فقد تمّ اختيار هاتين الحادثتين لأنهما معروفتان جداً وأثّرتا على مجموعة واسعة من المستهلِكين، ولكنّهما، وبسبب أوجه الفرْق في المعلومات التي تحتفظ بها كلّ منهما، قد تكون الاستجابات المستنبطة مختلفة منطقيّاً. ولكلّ من عمليتَي الاختراق، نسأل عن مدى قلق المستهلِكين وكيفية استجابتهم. في القسْم الثالث والأخير، كان الهدف فهْم كيفية احتمال استجابة المستهلِكين للسيناريوهات الافتراضية التي تنطوي على مستويات مختلفة من التهديدات على أمن معلوماتهم. ولتحقيق أكبر إمكانية للتطبيق والفهم بين المجيبين، قمنا بتصميم السيناريوهات الافتراضية حول عمليات اختراق الهواتف المحمولة. بعبارة أخرى، صمّمنا السيناريوهات حول ما وصفناه سابقاً بالخطر الناجم عن فك التشفير "الآنيّ" أي أنّ بإمكان حاسوب كمومي الحصول على المفتاح الخاص لهيئة إصدار شهادات جذر (root certificate authority) وإصدار شهادات رقمية قد تُعرِّف عن نفسها زيفاً بهدف تحميل برمجيات خبيثة والتحكم في الهواتف المحمولة. يفترض السيناريو الافتراضي الأول أنّ التكنولوجيا "شبه متطوّرة" وقد تسمح للقراصنة "بالتحكم في الهواتف الذكية" وأنّ "شركة تصنيع هاتفك الذكي ... لم تقم بتثبيت أنظمة أمن جديدة ولكن الشركات الأخرى قامت بذلك." يزيد السيناريو الافتراضي الثاني من قرب التهديد ويفترض أنّ "القراصنة يمتلكون التكنولوجيا للتحكم في الهواتف الذكية" و"لم تقم شركة تصنيع هاتفك الذكي بتثبيت أنظمة أمن جديدة." ويفترض السيناريو الافتراضي الأخير أن "القراصنة استخدموا التكنولوجيا الجديدة" و"يمكنهم الآن رؤية كلّ ما يوجد على هاتفك الذكي والتحكم فيه." يتراوح نطاق الاستجابات المحتملة لكلّ من هذه السيناريوهات ما بين الاحتفاظ بالهاتف الذكي واستخدامه بالطريقة نفسها وصولاً إلى التوقُّف تماماً عن استخدام الهواتف الذكية. راجِع الملحق D، المتوفّر على الموقع الإلكتروني: www.rand.org/pubs/research_reports/RR3102.html، للاطلاع على نص الدراسة الاستقصائية حول المستهلِكين.

خطة تحليل الدراسة الاستقصائية حول المستهلِكين

إنّ خطتنا لتحليل الدراسة الاستقصائية حول المستهلِكين وصفيّة. ففي خطوةٍ أولى، سنبيِّن مستوى الوعي العام بالحوسبة الكمومية، والقلق والاستجابات لعمليات اختراق الأمن الإلكتروني السابقة، والاستجابات المفاد بها للسيناريوهات الافتراضية التي تنطوي على مستويات مختلفة من التهديدات على الأمن الإلكتروني. بعد ذلك، سنستخدم المعلومات الديموغرافية التي تمّ جمعُها لتكون جزءاً من الدراسة الاستقصائية حول المستهلِكين لتوضيح كيفية اختلاف الاستجابات بحسب الجنس والعمر والمنطقة. وأخيراً، نستخدم تحليل الانحدار الوصفي كي نبيِّن كيفية ارتباط الاستجابات للسيناريوهات الافتراضية بالاستجابات لحوادث الأمن الإلكتروني السابقة، مستبعدين الديموغرافيات. قد يكون للتقديرات الناتجة عن تحليل الانحدار الوصفي هذا تداعيات مالية على المنظمات التي تحتفظ حالياً بمعلومات المستهلِكين الخاصّة.

الملاحظات

[1] من الناحية العملية، غالباً ما يتمّ الآن توليد المفاتيح ومشاركتها على الشبكات عن طريق إجراء تبادُل للمفاتيح العامة، مثل بروتوكول تبادُل مفتاح ديفي-هيلمان (Diffie-Helman key exchange protocol)، حيث غالباً ما يتمّ استخدام المفاتيح العامة قصيرة الأجل لإنشاء مفتاح متناظر مشترك بشكل آمن بين كيانين على شبكة.

[2] في حين يتمحور هذا التقرير حول تطبيقات التشفير، تجدر الإشارة إلى أنّ التطبيقات التجارية المتوقَّعة التي لا علاقة لها بالتشفير تُحفِّز قدراً كبيراً من الجهد المبذول لتطوير الحواسيب الكمومية. تتضمّن هذه التطبيقات على سبيل المثال لا الحصر تقدُّمات في المحاكاة والتحسين وأخْذ العينات الكمومية. راجِع محسني وآخرين (Mohseni et al.)، 2017، لمزيدٍ من التفاصيل حول التطبيقات التجارية الأخرى التي تدفع بالاستثمار في مجال الحوسبة الكمومية.

[3] نظرية فيزيائيّة أساسية تصِف طريقة تصرُّف الجُسَيمات عند نطاقات الأطوال الذرية ودون الذريّة.

[4] تشمل بعض هيئات إصدار المعايير البارزة التي تعمل في هذا المجال المعهد الأوروبي لمعايير الاتصالات (European Telecommunications Standards Institute)، وقطاع الاتصالات التابع للاتحاد الدولي للاتصالات (International Telecommunications Union Telecommunications Sector)، وفرِقة العمل المعنية بهندسة الإنترنت (Internet Engineering Task Force)، والمعهد الأمريكي للمعايير الوطنية (American National Standards Institute). واعتباراً من سبتمبر/أيلول 2018، يمكن العثور على ملخص مفيد عن هذه الجهود صادر عن شركة إيسارا (ISARA) في بيسن (Pecen) (2018).

[5] على الرغم من ذلك، قد تبقى كلّ المعلومات التي تمّ التقاطها قبل ذلك الانتقال ضعيفة في وجه الاختراقات اللاحقة عندما تُصبح قدرة الحوسبة الكمومية قائمة لمهاجمة التشفير باستخدام المفتاح العام (PKC) الذي يحمي البيانات المخزّنة.

[6] إننا نلاحظ أنّ هذا التعريف يتضمّن على الأقلّ مفهومين متتاليين مترابطين يتمّ تركهما غامضين عمداً: طول مفتاح تطبيق التشفير، وتعريف إطار زمني مفيد. سيزداد وقت التوصّل إلى حلٍّ بشكلٍ طبيعيٍّ مع زيادة طول المفتاح وينخفض مع تقدُّم قدرة الحوسبة. إننا نفترض أنّ هناك ما يكفي من عدم اليقين في التنبؤ بجدول بعض القدرات المستقبلية الزمني وبالتالي قد لا يكون التحديد الأدقّ لهذه المفاهيم أكثر إفادة.

[7] من الضروري التمييز بين البِتّات الكموميّة المنطقيّة *(logical qubits)* والبِتّات الكموميّة الماديّة *(physical qubits)* أو البوابات *(gates)*. عادةً ما تجِد تقديرات الموارد أنّ الحاجة ستدعو إلى آلاف البتات الكمومية المنطقية لإجراء هذه العمليات الحسابية وستكون هذه البتات الكمومية المنطقية مؤلَّفة من مئات الملايين من البِتات الكمومية الماديّة أو البوابات.

[8] قامت وكالة الأمن القومي (NSA) مؤخراً بإعادة تنظيم مديرية ضمان أمن المعلومات (IAD) وحلّها ونقْل عدد من أنشطتها إلى مديرية الأمن الإلكتروني (Cybersecurity Directorate) المُنشأة حديثاً.

[9] يمكن أيضاً ذكْر خوارزميات اتفاقية المفاتيح (key agreement algorithms) وخوارزميات التوقيع الرقمي (digital signature algorithms) هنا. وهي متميزة من الناحية الوظيفية عن الأساليب الأخرى التي تمت مناقشتها، وغالباً ما يتم استخدامها بالتضافر مع هذه الأساليب الأخرى في الاتصالات الحديثة عبر الإنترنت.

[10] لوصف هذا الأمر بطريقة أخرى قد يصح القول بأنّ هناك شهادة تتحقّق من أنّ مستخدِماً واحداً، وهذا المستخدِم وحده، يمتلك المفتاح الخاص المرتبط بمفتاحه العام.

[11] لمناقشة أكثر شموليّةً لتأثير الحوسبة الكمومية على التشفير الحالي، راجِع أعمال المعهد الأوروبي لمعايير الاتصالات (European Telecommunications Standards Institute [ETSI]) (2015) وشينك (Shenk) (2018).

[12] لاحِظ أنّه على عكْس الاعتقاد الشائع، لا تقوم الحواسيب الكمومية بهذا الأمر عن طريق "اختبار كلّ حلّ محتمل بشكل متزامن"، كما يتمّ وصْفه بشكل شائع. بدلاً من ذلك، تستخدِم عملية حسابية تسمّى "تحويل فورييه الكمومي" (quantum Fourier transform") لتحديد نمط في المفتاح، ما يتيح لمزيد من عمليات الحوسبة التقليدية استخراج المفتاح الخاص.

[13] لاحِظ أنّه يُطلق على هذا الأمر أحياناً مصطلح التقط الآن وفكّ التشفير لاحقاً *(catch now, decrypt later)*، ولكنّنا اعتمدنا هذا المصطلح بعد المناقشة مع براين لاماكيا (Brian LaMacchia) لأنه يشمل التهديد بشكل أكمل.

[14] تشير حزمة البروتوكولات *(protocol stack)* إلى طبقات البروتوكولات المختلفة التي تحكم أنشطة الشبكة المختلفة والتي يتفاعل البعض منها مع البعض الآخر لتشكيل بنية اتصالاتنا التحتية (ماك مايكل [MacMichael]، 2017).

[15] لاحِظ أنّه في بعض الأنظمة، يتمّ توليد مفاتيح مؤقتة لكلّ رسالة فردية، وليس لجلسة جديدة فحسب، ما قد يوفّر حماية إضافية.

[16] تشير شفافية الشهادة إلى أطر العمل التي تهدف إلى رصْد كيفية إصدار بعض الشهادات أو استخدامها والتدقيق فيها (جوجل [Google]، غير مؤرَّخ).

[17] ما لم تتمّ الإشارة إلى خلاف ذلك، فإن الجداول الزمنية المصوّرة هي نظريّة وتستند إلى دورات التطوير، ومعدلات الاعتماد، وأعمار المنتج المعقولة التقريبية، وفقاً لتقييم المؤلفَين. كما يفترض الشكل بتفاؤلٍ اعتماداً سريعاً للتشفير ما بعد الكمّ (PQC) في دورات تصميم المُنتَج على امتداد الصناعات.

[18] لاحِظ أنّ هذا الشكل يهدف إلى تصوير الضعف وليس الخطر في هذه المنتجات بمرور الوقت. أي أنّنا لا نناقش مدى أرجحيّة استغلال أي نقطة ضعْف أو ما قد تكون العواقب في مثل هذه الحالة.

[19] في حين دعت منظمات متعدّدة إلى اتخاذ تدابير بشأن الأمن الإلكتروني، فإن المجلس الاستشاري لاتصالات الأمن القومي (NSTAC) هو لجنة استشارية فيدرالية (Federal Advisory Committee) مرتبطة بالرئيس، مثل عدد قليل من هذه اللجان؛ يكون أعضاؤه من القطاع؛ وتتم إدارته من خلال وزارة الأمن الداخلي (Department of Homeland Security)، ممّا قد يجعل مثل هذا الجهد أكثر تأثيراً وفعاليةً بشكلٍ محتمل.

[20] في بعض الأحيان، سيشير الخبراء إلى أنّ أحدَث تقدير لديهم هو "بتاتاً" أو بعد "وقت طويل" غير محدَّد. ومن الواضح أن هذا الأمر يعود إلى أنّ هذا التقدير غير رقمي، وبالتالي لا يمكن دمجه مباشرةً في متوسط مرجّح. بهدف احتساب المتوسطات المرجحة بالاستناد إلى الخبرة في وجود هذه التقديرات غير الرقمية، قمنا بترميز وقت طويل على أنّه عام 2080 وبتاتاً على أنّه عام 2100.

[21] لاحِظ أنّ أرقام المقابلات في هذا الشكل والأشكال الأخرى المبيَّنة في هذا الفصل لا تتوافق مع المقابلة نفسها. تمّ تخصيص أرقام المقابلات بشكل عشوائي ومستقل لكلّ شكل للحفاظ على عدم نسْب أحكام الخبراء وعدم الكشف عن هويتهم.



Ablon, L., P. Heaton, D. C. Lavery, and S. Romanosky. (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*. Santa Monica, Calif.: RAND Corporation, RR-1187-ICJ. As of August 27, 2019: https://www.rand.org/pubs/research_reports/RR1187.html

Anschuetz, E. R., J. P. Olson, A. Aspuru-Guzik, and Y. Cao. (2018, August 27). "Variational Quantum Factoring." Cornell University. ArXiv Preprint.

Arute, Frank, et al. (2019, October). "Quantum Supremacy Using a Programmable Superconducting Processor." *Nature*, Vol. 574, pp. 505–510.

Ashford, W. (2018, August 23). "Cryptographic Agility Is Key to Post-Quantum Security." *Computer Weekly*. As of August 27, 2019: https://www.computerweekly.com/news/252447430/Cryptographic-agility-is-key-to-post-quantum-security

Aysu, A. (2018). "Post-Quantum Cryptography: From Theoretical Foundations to Practical Deployments." *Cryptography Special Issue*. As of August 27, 2019: https://www.mdpi.com/journal/cryptography/special_issues/Post_Quantum_Cryptography

Bernard, T. S., T. Hsu, N. Perlroth, and R. Lieber. (2017, September 7). "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." *New York Times*. As of August 27, 2019: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

Beurdouche, B., K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue. (2015). "A Messy State of the Union: Taming the Composite State Machines of TLS." *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, San Jose, Calif., May 17–21, 2015, pp. 535–552.

Bishop, L. S., S. Bravyi, A. Cross, J. M. Gambetta, and J. Smolin. (2017). *Quantum Volume*. Technical report.

Bleicher, A. (2018, February 1). "Quantum Algorithms Struggle Against Old Foe: Clever Computers." *Quanta Magazine*.

Bright, P. (2018, October 16). "Apple, Google, Microsoft, and Mozilla Come Together to End TLS 1.0." *Ars Technica* blog. As of August 28, 2019: https://arstechnica.com/gadgets/2018/10/browser-vendors-unite-to-end-support-for-20-year-old-tls-1-0/

Campbell, L. (2018, April 18). "Worse than Y2K: Quantum Computing and the End of Privacy." *Forbes*. As of August 28, 2019: https://www.forbes.com/sites/forbestechcouncil/2018/04/18/worse-than-y2k-quantum-computing-and-the-end-of-privacy/

Campbell, P., M. Groves, and D. Shepherd. (2014). *Soliloquy: A Cautionary Tale*. Cheltenham, UK: Government Communications Headquarters.

Chang, L., and J. A. Krosnick. (2009, Winter). "National Surveys via RDD Telephone Interviewing Versus the Internet: Comparing Sample Representativeness and Response Quality." *Public Opinion Quarterly*, Vol. 73, No. 4, pp. 641–678.

Chen, L., S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. (2016). *Report on Post-Quantum Cryptography*. NISTIR 8105. Gaithersburg, Md.: National Institute of Standards and Technology.

"Chinese Satellite Uses Quantum Cryptography for Secure Video Conference Between Continents." (2018, January 30). *Technology Review*. As of August 28, 2019: https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/

CISA—*See* Cybersecurity and Infrastructure Security Agency.

Clemen, R. T., and R. L. Winkler. (2007). "Aggregating Probability Distributions." In W. Edwards, R. F. Miles, Jr., and D. von Winterfeldt, eds., *Advances in Decision Analysis: From Foundations to Applications*, Cambridge, UK: Cambridge University Press, pp. 154–176.

Colson, A. R., and R. M. Cooke. (2018, February 2). "Expert Elicitation: Using the Classical Model to Validate Experts' Judgments." *Review of Environmental Economics and Policy*, Vol. 12, No. 1, pp. 113–132.

Committee on National Security Systems. (2015). "Use of Public Standards for the Secure Sharing of Information Among National Security Systems." Advisory Memorandum 02-15. Ft. Meade, Md.

Cooke, R. M., and Goossens, L. L. (2008, May). "TU Delft Expert Judgment Data Base." *Reliability Engineering and System Safety*, Vol. 93, No. 5, pp. 657–674.

Curtright, A. E., M. G. Morgan, and D. W. Keith. (2008, November 14). "Expert Assessments of Future Photovoltaic Technologies." *Environmental Science and Technology*, Vol. 42, No. 24, pp. 9031–9038.

Cybersecurity and Infrastructure Security Agency. (Undated). "What Does CISA Do?" Homepage. U.S. Department of Homeland Security. As of February 11, 2020: https://www.cisa.gov/

Encryption Working Group. (2019). *Implications of Quantum Computing for Encryption Policy*. Center for Information Technology Policy. Washington, D.C.: Carnegie Endowment for International Peace.

European Telecommunications Standards Institute. (2015, June). "Quantum Safe Cryptography and Security." White paper. Sophia Antipolis, France.

ETSI—*See* European Telecommunications Standards Institute.

Foremski, T. (2018, May 18). "IBM Warns of Instant Breaking of Encryption by Quantum Computers: 'Move Your Data Today.'" *ZDNet*. As of September 3, 2019: https://www.zdnet.com/article/ibm-warns-of-instant-breaking-of-encryption-by-quantum-computers-move-your-data-today/

Friedman, S. (2018, March 1). "DoD's Growing Interest in Quantum and Blockchain." *GCN*. As of September 4, 2019: https://gcn.com/Articles/2018/03/01/DOD-quantum-blockchain.aspx

GAO—*See* U.S. Government Accountability Office.

General Services Administration. (2018). "Information Technology Strategic Plan: FY2018–2020." Washington, D.C.

Google. (Undated.) "Certificate Transparency." Webpage. As of August 29, 2019: https://www.certificate-transparency.org/

Grover, L. K. (1996). "A Fast Quantum Mechanical Algorithm for Database Search." *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, Philadelphia, Pa., May 22–24, 1996, pp. 212–219.

Morgan, M. G., and M. Henrion. (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. New York: Cambridge University Press.

Morgan, M. G., L. F. Pitelka, and E. Shevliakova. (2001). "Elicitation of Expert Judgments of Climate Change Impacts on Forest Ecosystems." *Climatic Change*, Vol. 49, No. 3, pp. 279–307.

Mosca, M. (2015). "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IACR Cryptology ePrint Archive, p. 1075.

Mosca, M., and J. Mulholland. (2017). *A Methodology for Quantum Risk Assessment*. Toronto: Global Risk Institute.

Moses, T. (2009). "Quantum Computing and Cryptography." Entrust, Inc., Addison, Texas.

Moskvitch, K. (2018, February 7). "The Argument Against Quantum Computers." *Quanta Magazine*.

Mulvaney, M. (2018). "Implementation of the Modernizing Government Technology Act." Memorandum M-18-12. Washington, D.C.: Office of Management and Budget.

NAS—*See* National Academies of Sciences, Engineering, and Medicine..

National Academies of Sciences, Engineering, and Medicine. (2018a). "Cryptographic Agility and Interoperability: Proceedings of a Workshop." *Proceedings of the Forum on Cyber Resilience Workshop*. Washington, D.C.: National Academies Press, p. 90.

———. (2018b). *Quantum Computing: Progress and Prospects*. Washington, D.C.: National Academies Press.

National Cyber Security Centre. (2016, November 30). "Quantum Key Distribution." White paper. As of August 28, 2019: https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution

National Institute of Standards and Technology. (2001). "Announcing the Advanced Encryption Standard." FIPS Pub 197. Gaithersburg, Md.

———. (2002). "Secure Hash Standard." FIPS Pub 180-2. Gaithersburg, Md.

———. (2016a). "NIST Cryptographic Standards and Guidelines Development Process." NISTIR 7977. Gaithersburg, Md.

———. (2016b, December 20). "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms." Press release. As of August 28, 2019: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms

———. (2017, January 3). "Post-Quantum Cryptography." Webpage. As of August 28, 2019: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

———. (2018a). "Framework for Improving Critical Infrastructure Security." Gaithersburg, Md. As of February 11, 2020: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

———. (2018b, September 4). "Post-Quantum Cryptography: Workshops and Timeline." As of August 28, 2019: https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

GSA—*See* General Services Administration.

IAD—*See* Information Assurance Directorate.

IETF—*See* Internet Engineering Task Force.

Information Assurance Directorate. (2016). "Commercial National Security Algorithm Suite and Quantum Computing FAQ". Fact sheet. National Security Agency, Washington, D.C.

Internet Engineering Task Force. (1999). "The TLS Protocol: Version 1.0." Memorandum.

Internet Society. (2018, June 6). "State of IPv6 Deployment 2018." Webpage. As of August 28, 2019: https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

Kalai, G. (2016). "The Quantum Computer Puzzle." *Notices of the AMS*, Vol. 63, No. 5, pp. 508–516.

Keeter, S., and L. Christian. (2012, November 7.) *A Comparison of Results from Surveys by the Pew Research Center and Google Consumer Surveys*. Washington, D.C.: Pew Research Center.

Knol, A. B., J. J. de Hartog, H. Boogaard, P. Slottje, J. P. van der Sluijs, E. Lebret, F. R. Cassee, J. A. Wardekker, J. G. Ayers, P. J. Borm, B. Brunekreef, K. Donaldson, F. Forastiere, S. T. Holgate, W. G. Kreyling, B. Nemery, J Pekkanen, V. Stone, H.-E. Wichmann, and G. Hoek. (2009). "Expert Elicitation on Ultrafine Particles: Likelihood of Health Effects and Causal Pathways." *Particle and Fibre Toxicology*, Vol. 6, No. 19.

Lavrakas, P. J. (2010). *An Evaluation of Methods Used to Assess the Effectiveness of Advertising on the Internet*. New York: Interactive Advertising Bureau.

Lee, T. B. (2017, May 15). "The WannaCry Ransomware Attack Was Temporarily Halted. But It's Not over Yet." *Vox*. As of August 28, 2019: https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp

Leech, D. P., S. Ferris, and J. T. Scott. (2018). *The Economic Impacts of the Advanced Encryption Standard,1996–2017*. NIST GCR 18-017. Gaithersburg, Md.: National Institute of Standards and Technology.

Lew, J. J. (2011). "Chief Information Officer Authorities." Memorandum M-11-29. Office of Management and Budget, Washington, D.C.

Leyden, J. (2017, September 5). "Bazinga! Social Network Taringa 'Fesses up to Data Breach." *The Register*. As of August 28, 2019: https://www.theregister.co.uk/2017/09/05/taringa_data_breach/

MacMichael, D. (2017, April 19). "Windows Network Architecture and the OSI Model." Webpage. Microsoft. As of August 28, 2019: https://docs.microsoft.com/en-us/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model

McDonald, P., M. Mohebbi, and B. Slatkin. (2012). *Comparing Google Consumer Surveys to Existing Probability and Non-Probability Based Internet Surveys*. Mountain View, Calif.: Google Inc.

Mohseni, M., P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A. Fowler, V. Smelyanskiy, and J. Martinis. (2017). "Commercialize Quantum Technologies in Five Years." *Nature*, Vol. 543, No. 7644, pp. 171–175.

Morgan, M. G. (2014). "Use (and Abuse) of Expert Elicitation in Support of Decision Making for Public Policy." *Proceedings of the National Academies of Sciences*, pp. 7176–7184.

Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, N.M. , November 22–24, 1994, pp. 124–134.

Smith, Aaron, and Monica Anderson. (2018, March 1). *Social Media Use in 2018*. Washington, D.C.: Pew Research Center.

Sotirov, A., M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. D. Weger. (2008, December 30). "MD5 Considered Harmful Today: Creating a Rogue CA Certificate." Presented at 25th Annual Chaos Communication Congress, Berlin, 2008. As of August 28, 2019:
http://www.win.tue.nl/hashclash/rogue-ca/

Stiennon, R. (2012, June 14). "Flame's MD5 Collision Is the Most Worrisome Security Discovery of 2012." *Forbes*. As of August 28, 2019:
https://www.forbes.com/sites/richardstiennon/2012/06/14/flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/

Subcommittee on Quantum Information Science. (2018). *National Strategic Overview for Quantum Information Science*. Washington, D.C.: National Science and Technology Council.

Sullivan, N. (2017, December 26). "Why TLS 1.3 Isn't in Browsers Yet." *Cloudflare* blog. As of August 28, 2019:
https://blog.cloudflare.com/why-tls-1-3-isnt-in-browsers-yet/

Thales eSecurity. (2018). "FAQ." Webpage. As of August 28, 2019:
https://www.thalesesecurity.com/faq

Touzalin, A. (2016, May). "Quantum Manifesto: A New Area of Technology."

Tversky, A., and D. Kahneman. (1974). "Judgment Under Uncertainty: Heuristics and Biases." *Science*, Vol. 185, No. 4157, pp. 1124–1131.

U.S. Code, Title 15, Sections 8801–8852, National Quantum Initiative Act.

U.S. Government Accountability Office. (2000). "Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges." Washington, D.C.

———. (2016). "Federal Agencies Need to Address Aging Legacy Systems." Washington, D.C.

U.S. Securities and Exchange Commission. (1999, September 17). Speech by SEC Chairman: Remarks to the President's Council on Year 2000 Conversion. Washington, D.C. As of August 28, 2019:
https://www.sec.gov/news/speech/speecharchive/1999/spch297.htm

"Venafi Research: 35 Percent of Websites Are Still Using Insecure SHA-1 Certificates and Putting Users at Risk." (2016, November 17). *Business Wire*. As of August 28, 2019:
https://www.businesswire.com/news/home/20161117005247/en/Venafi-Research-35-Percent-Websites-Insecure-SHA-1

Wallace, G. (2013, December 23). "Target Credit Hack: What You Need to Know." CNN Business. As of August 28, 2019:
https://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html

Weber, R. E. (2013). *Masked Dispatches: Cryptograms and Cryptology in American History, 1775–1900*. Fort Meade, Md: National Security Agency Center for Cryptologic History.

Wolchover, N. (2015, September 8). "A Tricky Path to Quantum-Safe Encryption." *Quanta Magazine*. As of August 28, 2019:
https://www.quantamagazine.org/quantum-secure-cryptography-crosses-red-line-20150908

———, (2018c, September 28). IST Launches Consortium to Support Development of Quantum Industry. As of February 24, 2020:
https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry

———. (2019). "Security Requirements for Cryptographic Modules." FIPS Pub 140-3. Gaithersburg, Md.

National Security Agency. (2016, April 12). "About IAD." Webpage. As of August 28, 2019:
https://apps.nsa.gov/iad/about/

National Security Telecommunications Advisory Committee. (2018). *NSTAC Report to the President on a Cybersecurity Moonshot*. Washington, D.C.: U.S. Department of Homeland Security.

NIST—*See* National Institute of Standards and Technology.

NSA—*See* National Security Agency.

NSTAC—*See* National Security Telecommunications Advisory Committee.

Office of Management and Budget. (2018). "Office of Management and Budget." Webpage. As of August 28, 2019:
https://www.whitehouse.gov/omb/

OMB—*See* Office of Management and Budget.

Pecen, M. (updated 2019, May 29). "Standards Update: Quantum-Safe Cryptography." Webpage. ISARA Corporation. As of August 28, 2019:
https://www.isara.com/standards/

Pew Research Center. (2011). "Collecting Survey Data." Webpage. As of September 11, 2019:
https://www.pewresearch.org/methods/u-s-survey-research/collecting-survey-data/#the-problem-of-declining-response-rates

Porges, S. (2015, December 6). "How to Design a New Car in 7 Steps." *Forbes*. As of August 28, 2019:
https://www.forbes.com/sites/sethporges/2015/12/06/these-are-the-7-steps-it-takes-to-design-a-new-auto-product/

PQCrypto. (2018). "PQCrypto 2019." Webpage. As of August 28, 2019:
http://pqcrypto2019.org/

Quantum Xchange. (2018). "Quantum Safe Security in a 5G World." Webpage. As of August 28, 2019:
https://quantumxc.com/quantum-safe-security-in-a-5g-world/

Roetteler, M., M. Naehrig, K. M. Svore, and K. Lauter. (2017). "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms." *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Hong Kong, December 3–7, 2017.

Rowe, G., and G. Wright. (1999). "The Delphi Technique As a Forecasting Tool: Issues and Analysis." *International Journal of Forecasting*, Vol. 15, No. 4, pp. 353–375.

Santoso, L. P., R. Stein, and R. Stevenson. (2016, Summer). "Survey Experiments with Google Consumer Surveys: Promise and Pitfalls for Academic Research in Social Science." *Political Analysis*, Vol. 24, No. 3, pp. 356–373.

SEC—*See* U.S. Securities and Exchange Commission.

Shenk, M. (2018). *The Quantum Countdown: Quantum Computing and the Future of Smart Ledger Encryption*. Zug, Switzerland: Cardano Foundation.

Wolf, M., and T. Gendrullis. (2011). "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module." *Proceedings of the International Conference on Information Security and Cryptology*, Seoul, South Korea, November 30–December 2, 2011, pp. 302–318.

Yerukhimovich, A., R. Balebako, A. Boustead, R. K. Cunningham, W. Welser IV, R. Housley, R. Shay, C. Spensky, K. D. Stanley, J. Stewart, A. Trachtenberg, and Z. Winkelman. (2016). *Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and IOS Devices*. Santa Monica, Calif: RAND Corporation, RR-1393-DARPA. As of August 28, 2019:
https://www.rand.org/pubs/research_reports/RR1393.html

Zalka, C. (1999, October 1). "Grover's Quantum Searching Algorithm Is Optimal." *Physical Review A*, pp. 2746–2751.

Zickfield, K., A. Levermann, M. G. Morgan, T. Kuhlbrodt, S. Rahmstorf, and D. W. Keith. (2007). "Expert Judgments on the Response of the Atlantic Merdional Overturning Circulation to Climate Change." *Climatic Change*, Vol. 82, No. 3–4, pp. 235–265.

عن مركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security)

يعمل مركز المخاطر والأمن العالمي (RAND Center for Global Risk and Security [CGRS]) على امتداد مؤسسة RAND لتطوير أبحاث متعددة الاختصاصات وتحليل السياسات التي تتناول المخاطر المنهجية على الأمن العالميّ. يعتمد المركز على خبرة مؤسسة RAND لاستكمال أبحاث RAND وتوسيعها في مجالات متعدّدة، بما في ذلك الأمن، والاقتصاد، والصحة، والتكنولوجيا. يقدم مجلس مؤلَّف من كبار قادة الأعمال المتميزين والمحسنين وصانعي السياسات السابقين المشورة والدعم لأنشطة المركز، التي تركِّز بشكلٍ متزايدٍ على اتجاهات الأمن العالمي وتأثير التكنولوجيات التعطيلية على المخاطر والأمن. لمزيدٍ من المعلومات حول مركز RAND للمخاطر والأمن العالميّ، يرجى زيارة الموقع الإلكتروني: .www.rand.org/international/cgrs

شكر وعِرفان

نود أن نشكر كبار مستشارينا، وهم براين جاكسون (Brian Jackson)، ومارجوري بلومنثال (Marjory Blumenthal)، وريبيكا بالباكو (Rebecca Balebako) على توجيهاتهم خلال هذا المشروع البحثي. فقد كانت رؤيتهم قيّمة وساهَمَت في إنجاز المشروع بنجاح. إننا نقِّر بالامتنان لكلّ الذين قابلناهم طوال هذا الجهد للوقت الذي خصّصوه لإنارة عملنا. نود أيضاً أن نشكر مركز RAND للمخاطر والأمن العالميّ (RAND Corporation Center for Global Risk and Security) على دعمه لهذا البحث. وبالتحديد، إننا نشكر أندرو باراسيليتي (Andrew Parasiliti)، وروبن ميلي (Robin Meili). كما نشكر أيضاً سوني إيفرون (Sonni Efron)، وغريغوري بومان (Gregory Baumann)، وإيرين سميث (Erin Smith) على دعمهم في إعداد هذا التقرير. وأخيراً، نشكر إدوارد (تيدي) باركر (Edward [Teddy] Parker) وتشاد أولاندت (Chad Ohlandt) من مؤسسة RAND ونيكولاس سوليفان (Nicholas Sullivan) من شركة كلاودفلار (Cloudflare, Inc)، للعمل بصفتهما مراجعَين.

عن المؤلِفين

مايكل ج. د. فيرمير (Michael J.D. Vermeer) هو عالِم فيزيائي في مؤسسة RAND. تركِّز أبحاثه على سياسات العلوم والتكنولوجيا، والعدالة الجنائية، والأمن القومي، والتكنولوجيات الناشئة والابتكارات. تشمل أبحاثه الأخيرة السياسات والإجراءات والاحتياجات التكنولوجية لوكالات العدالة الجنائية، والتخطيط للتطوير وتقييم البرامج للخدمات العسكرية، وتداعيات مختلف التكنولوجيات الناشئة على الأمن القومي. لقد حاز شهادة البكالوريوس في العلوم من كلية كالفن (Calvin College) وشهادة الدكتوراه من جامعة نورث وسترن (Northwestern University).

إيفان د. بيت (Evan D. Peet) هو عالِم اقتصادي في مؤسسة RAND. تركِّز أبحاثه على الاقتصاد الجزئي التطبيقي الذي يتناول مجالات الصحة ورأس المال البشري والأمن. طوّر من خلال أبحاثه أساليب جديدة تستفيد من البيانات الضخمة للتنبؤ بخطر نتائج الصحّة السيئة، وتحديد التدخّلات التي تحدّ من الخطر. بالإضافة إلى ذلك، قام بنمذجة تكاليف التدابير الهادِفة إلى منْع وقوع الصراعات الأمنية وفوائدها والتي تمّ تطبيقها في مجموعة متنوعة من السياقات. لقد حاز شهادة الدكتوراه في الاقتصاد من جامعة ديوك (Duke University) عام 2013 وأكمل برنامج الزمالات ما بعد الدكتوراه في جامعة هارفارد (Harvard University) قبل انضمامه إلى مؤسسة RAND عام 2015.

عن هذا التقرير

تعِد تكنولوجيا الحوسبة الكمومية الناشئة بتوفير قدرات حوسبة جديدة وقوية، ولكنّها تشكّل أيضاً تهديداً محتملاً لبنية اتصالاتنا التحتية. من المتوقَّع بشكل كبير أن يكون لوسائلنا لضمان أمن الاتصالات عبر الإنترنت في شكلها الحالي، أي بالتشفير باستخدام المفتاح العام، نقاط ضعْف قد تستغِلّها الحوسبة الكمومية. يتمّ تطوير أشكال جديدة من التشفير باستخدام المفتاح العام والتي يُتوقَّع أن تكون آمنة، ولكنْ، إن لم تُستخدَم على نطاق واسع في الوقت الذي تظهر فيه الحواسيب الكمومية، الواسعة النطاق، قد نتوقّع نقاط ضعف إلكترونية تعطيلية.

لقد تمّ استخدام مقاربة بحثيّة مختلطة الأساليب لتقييم المخاطر ووضْع توصيات في السياسات. على الرغم من وجود اختلاف كبير في تقييمات الخبراء، من المرجّح أن تنوجِد الحواسيب الكمومية القادرة على اختراق التشفير الحالي قبل أن تكون بنية الاتصالات التحتية الأمريكية مستعِدّة بالكامل. علاوةً على ذلك، سينمو الخطر كلّما طال انتظار المنظمات للانتقال إلى التشفير الجديد. بشكلٍ عام، تمّ تقييم التهديد الناجم عن الحوسبة الكمومية على أنّه ملحّ، وأنّ التدابير السريعة ضروريّة للحدّ من الخطر. يُعتبر برنامج مبادرة الكمّ الوطنية (National Quantum Initiative Program) الذي بدأ مؤخراً خطوةً أولى مهمة، ولكن يتوجّب على الحكومة الأمريكية اتّخاذ تدابير إضافية. يوصي المؤلفان بأن تضمن السلطة التنفيذية إيلاء أولوية كافية لهذه القضية وأن تبدأ هيئة التنسيق المختارة بتنظيم العمل على امتداد الحكومة الفيدرالية. يتوجب على الكونغرس أيضاً أن ينظر في بدء عقْد جلسات استماع للإشراف على جهود توحيد المعايير والانتقال. وأخيراً، يجب على المنظمات الفردية اتّخاذ خطوات بهدف الاستعداد لعملية الانتقال إلى التشفير القادمة وتكييف أنظمتها لدمج سرعة تشفير أكبر.

مبادرة مؤسسة RAND للأمن 2040 (Security 2040)

يُعَدّ هذا التقرير جزءاً من مبادرة مؤسسة RAND لتصَوُّر التحديات الأمنية الأساسيّة في عالَم العام 2040، مع الأخذ في عين الاعتبار آثار الاتجاهات السياسية والتكنولوجية والاجتماعية والديموغرافية التي ستشكِّل تلك التحديات الأمنية في العقود القادمة. لقد تمّ إجراء البحث في مركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security).

التمويل

لقد تمّ توفير التمويل لهذا المشروع من خلال الهبات من الجهات الداعمة لمؤسسة RAND وإيرادات العمليات.



تعِد تكنولوجيا الحوسبة الكمومية الناشئة بتوفير قدرات حوسبة جديدة وقوية، ولكنّها تشكّل أيضاً تهديداً محتملاً لبنية اتصالاتنا التحتية. من المتوقَّع بشكل كبير أن يكون لوسائلنا لضمان أمن الاتصالات عبر الإنترنت في شكلها الحالي، أي بالتشفير باستخدام المفتاح العام، نقاط ضعْف قد تستغِلّها الحوسبة الكمومية. يتمّ تطوير أشكال جديدة من التشفير باستخدام المفتاح العام والتي يُتوقَّع أن تكون آمنة، ولكنْ، إن لم تُستخدَم على نطاق واسع في الوقت الذي تظهر فيه الحواسيب الكمومية، الواسعة النطاق، قد نتوقّع نقاط ضعف إلكترونية تعطيلية.

لقد تمّ استخدام مقاربة بحثيّة مختلطة الأساليب لتقييم المخاطر ووضْع توصيات في السياسات. على الرغم من وجود اختلاف كبير في تقييمات الخبراء، من المرجّح أن تتوجِد الحواسيب الكمومية القادرة على اختراق التشفير الحالي قبل أن تكون بنية الاتصالات التحتية الأمريكية مستعِدّة بالكامل. علاوةً على ذلك، سينمو الخطر كلّما طال انتظار المنظمات للانتقال إلى التشفير الجديد. بشكلٍ عام، تمّ تقييم التهديد الناجم عن الحوسبة الكمومية على أنّه ملحّ، وأنّ التدابير السريعة ضروريّة للحدّ من الخطر. يُعتبر برنامج مبادرة الكمّ الوطنية (National Quantum Initiative Program) الذي بدأ مؤخراً خطوةً أولى مهمة، ولكن يتوجّب على الحكومة الأمريكية اتّخاذ تدابير إضافية. يوصي المؤلفان بأن تضمن السلطة التنفيذية إيلاء أولوية كافية لهذه القضية وأن تبدأ هيئة التنسيق المختارة بتنظيم العمل على امتداد الحكومة الفيدرالية. يتوجب على الكونغرس أيضاً أن ينظر في بدء عقْد جلسات استماع للإشراف على جهود توحيد المعايير والانتقال. وأخيراً، يجب على المنظمات الفردية اتّخاذ خطوات بهدف الاستعداد لعملية الانتقال إلى التشفير القادمة وتكييف أنظمتها لدمج سرعة تشفير أكبر.

www.rand.org

Arabic Translation of:
"Securing Communications in the Quantum Computing Age"
RR-3102/2-RC